CYBER ATTACK DETECTION SYSTEM FOR BIOMETRIC

Sharmila Kumari M.[1*], Afrah Abdul Aziz.[1], Disha D Naik.[1], Fareeha Faiz Ahsan.[1], Bhagyashree K.[1]

[1]Department of Computer Science and Engineering, P. A. College of Engineering, Mangaluru, Karnataka, India.

*Corresponding Author: Sharmila Kumari M Email: hod.cs@pace.edu.in

Abstract:

Biometric authentication has become integral in securing applications, enabling access to personal devices, and conducting secure transactions. However, it is susceptible to presentation attacks, particularly in the case of face recognition. This research proposes a novel system designed to detect and mitigate vulnerabilities associated with face-based biometric authentication. The primary objective of this work is to develop a robust and efficient solution for face presentation attack detection. It leverages a two-stream convolutional neural network (CNN) model, extracting patch-based features and full depth maps from face images. To enhance accuracy, feature engineering is integrated with the two- stream CNN model. Notably, this system is realized as a mobile application, allowing for the capture of face videos and seamless background execution. Authentic users can unlock their mobile devices and perform secure tasks, such as financial transactions. The proposed system stands out by its superior computational efficiency, robustness, and accuracy, making it a valuable addition to the biometric security landscape. Moreover, this research considers the unique characteristics of the Indian ethnic community by creating a tailored database. The potential applications of this system extend to educational institutions, local banks, and cooperative societies, showcasing its versatility and real- world relevance.

Key Words: Authentication, Face Presentation Attack Detection, Convolutional Neural Networks, Mobile Application Security, Ethnicity-based Database

ISBN-978-81-19905-39-3

1. Introduction

Human faces play a crucial role in our daily lives, especially in identifying people. Face recognition is a type of biometric identification in which facial features are extracted and stored as a unique face print to identify a person. In today's networked world, protecting information or physical property is becoming increasingly crucial and complex. We occasionally hear about credit card fraud, hacker attacks on computers, or security breaches at businesses or government buildings. Most of these crimes exploited a fundamental shortcoming in traditional access control systems: the systems provide access based on "what we have," such as ID cards, keys, passwords, PIN numbers, or mother's maiden name, rather than "who we are." None of these things truly define us. Recently, technology has become accessible that allows the authentication of "true" individual identity. This technology is based on an area called "biometrics". Biometric access control are automated means of authenticating or recognizing the identity of a living individual based on certain physiological traits, such as Fingerprints, facial traits, or components of a person's behavior, such as handwriting or keyboard patterns. Biometric systems are difficult to forge since they identify people based on their biological traits. Face recognition is one of the rare biometric technologies that combines high accuracy with little intrusiveness. It is as accurate as a physiological technique while remaining non-intrusive. As a result, since the early 1970s (Kelly, 1970), face recognition has piqued the interest of academics ranging from security, psychology, and image processing to computer vision.

2. Literature Review

Cybersecurity is a major issue in our digital world, while cybercrime is increasing. The banking and finance sectors have started to rely on biometric security systems for their apps and services. This review by Elhaam Abdulrahman Debas et al. [1] highlighted Biometric identification uses unique human characteristics to authenticate a person's identity, such as voice/speech recognition, fingerprint recognition, facial recognition, iris recognition, signature dynamics, etc. Biometric technology is used in banking, e-commerce, account login, access control, etc, which can be considered a valuable measure against cybercrime. Biometrics is a key to the future of cybersecurity and safeguards against cybercrime. Face anti-spoofing is a very critical step before

ISBN-978-81-19905-39-3

feeding the face image to biometric systems. In this work [2] authors proposed a novel two-stream CNN-based approach for face anti-spoofing, by extracting the local features and holistic depth maps from the face images. The local features facilitate CNN to discriminate the spoof patches independent of the spatial face areas. On the other hand, holistic depth map examines whether the input image has a face-like depth. Despite the potential of deep learning models to enhance vulnerability identification, the study highlights challenges such as high false positive and false negative rates that need to be addressed for improved accuracy in cyber security attack detection [3]. With the wide deployment of the face recognition systems in applications from deduplication to mobile device unlocking, security against the face spoofing attacks requires increased attention; such attacks can be easily launched via printed photos, video replays, and 3D masks of a face [4].In this work the problem of face spoof detection against the print and replay attacks based on the analysis of image distortion are addressed. As a result of COVID-19, 64% have increased prioritization for technology that supports remote onboarding and mobile apps. More than 90% of respondents said that liveness. This survey was provided by R. Tolosana et. al. [6] discussed techniques for manipulating face images including Deepfake methods, and methods to detect such manipulations. Four types of facial manipulation are reviewed: entire face synthesis, identity swap, attribute manipulation, and expression swap. For each manipulation group, provided details regarding manipulation techniques, existing public databases, and key benchmarks for technology evaluation of fake detection methods, including a summary of results from those evaluations.

The main contribution of this survey by Kotli, Y [7] is to review some well-known techniques for each approach and to give the taxonomy of their categories. A detailed comparison between these techniques is presented by listing the advantages and the disadvantages of their schemes in terms of robustness, accuracy, complexity, and discrimination. One interesting feature mentioned in the paper is the database used for face recognition. Lazarini et al. [8] proved the accuracy of face recognition algorithms, focusing on three key components: face detection, feature extraction, and facial recognition. The researchers found that the Viola-Jones algorithm is commonly used for face detection, while eigenface and fisherface methods based on Principal Component Analysis (PCA) are popular for feature extraction. Convolutional Neural Networks (CNNs) have emerged as the dominant approach for facial recognition tasks. However, the review also identified several

ISBN-978-81-19905-39-3

limitations in the current state of face recognition technology. One key issue is the lack of standardized evaluation metrics, making it challenging to compare the performance of different algorithms across studies. Additionally, the researchers noted that the accuracy of face recognition can be affected by biases in the training datasets, leading to uneven performance across demographic groups. Another significant concern is the ethical and privacy implications of face recognition technology, as it can be used for surveillance and other purposes without the consent of individuals. In the research paper [9] delves into various techniques for managing face identity threats. The study focuses on face detection, feature extraction, and pattern matching methods to enhance face recognition systems. Specifically, the paper discusses the utilization of Multi-task Cascaded Convolutional Networks for face detection, Principal Component Analysis (PCA) and Local Binary Patterns for feature extraction, and k-Nearest Neighbors, Support Vector Machines, and Convolutional Neural Networks for pattern matching. However, the research has been critiqued for not providing detailed attention to Direct Spoofing, Zero Effort Imposter, and Intrinsic Factors, potentially leaving gaps in addressing these specific threats effectively. Moreover, the paper lacks a comprehensive outline of countermeasures for these challenges, which could limit the practical applicability of the proposed techniques. Additionally, the study falls short in exploring potential drawbacks or limitations associated with Scattered-CNN and Multi-Task-CNN, which are crucial for understanding the overall effectiveness and reliability of the proposed methods. Smith M and Seumas Miller S. [10] examined the rise of biometric facial recognition, current applications and legal developments, and conducted an ethical analysis of the issues that arise. Ethical principles are applied to mediate the potential conflicts in relation to this information technology that arise between security, on the one hand, and individual privacy and autonomy, and democratic accountability, on the other. These can be used to support appropriate law and regulation for technology as it continues to develop. The work is proposed [11], and a real-time laboratory setup is performed to capture network packets and examine this captured data using various DL techniques. A comparable interpretation is presented under the DL techniques with essential parameters, particularly accuracy, false alarm rate, precision, and detection rate. The DL techniques experimental output projects improvise the performance of various real-time cybersecurity applications on a real-time dataset. CNN model provides the highest accuracy. The RNN model

ISBN-978-81-19905-39-3

offers the second-highest accuracy. CNN model provides the highest accuracy of 98.42 with multiclass class. The study shows that DL techniques can be effectively used in cybersecurity applications.

3. Proposed Methodology

A thorough survey has shown that different approaches, as well as combinations of these approaches, can be used to create a new face recognition system. We have chosen to combine knowledge-based techniques for face detection and neural network techniques for face recognition among the many other available ways.

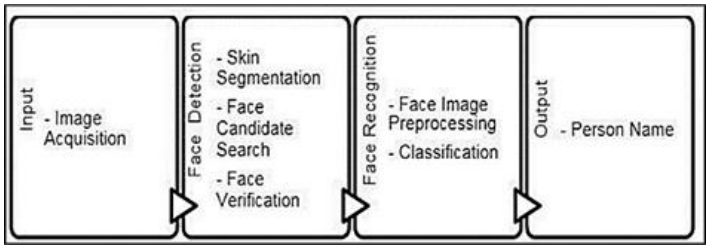

Fig. 1: Face Recognition Approach

The system architecture of the proposed facial recognition system comprises two key components: face detection and face recognition. At the core of the architecture lies the integration of knowledge-based techniques for face detection and neural network techniques for face recognition. This hybrid approach leverages the strengths of both methodologies, ensuring robust performance and high accuracy. The face detection component utilizes the Haar cascade classifier, a widely used algorithm known for its efficiency in identifying facial features. Initially, the system captures a color image from the camera and converts it to grayscale. Subsequently, the Haar cascade classifier is applied to detect faces within the image. Upon detection, facial landmarks are analyzed, and a square frame is drawn around each detected face, enabling precise identification. In parallel, the face recognition component employs Convolutional Neural Networks (CNNs), a deep learning technique renowned for its ability to extract intricate patterns and features from images. Trained on a custom dataset comprising diverse facial images, CNN learns to discern unique facial characteristics and associations. When presented with a new face image, the CNN processes the

ISBN-978-81-19905-39-3

input through its layers, extracting features and comparing them with learned patterns. This comparison allows the system to accurately recognize and identify individuals, even amidst variations in lighting, pose, or facial expressions. The seamless integration of these components ensures a comprehensive and efficient facial recognition system capable of real-time operation. By combining knowledge- based and neural network techniques, the architecture maximizes accuracy and reliability, making it suitable for diverse applications ranging from access control to attendance management. Moreover, the modular design of the architecture facilitates scalability and future enhancements, ensuring adaptability to evolving requirements and technological advancements. Figure 2 shows Workflow of facial recognition.

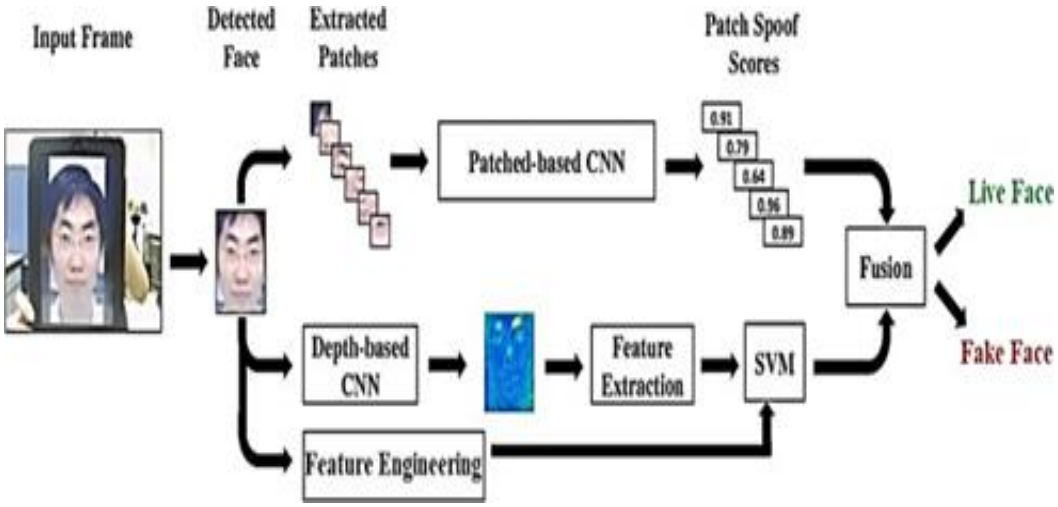

Fig. 2: Workflow of facial recognition

The system incorporates an Image Processing Module, which utilizes OpenCV for efficient face detection and preprocessing of images. This module plays a crucial role in identifying facial features accurately, providing a foundation for subsequent processing. Following detection, the Face Recognition Module comes into play, employing a machine learning model to analyze facial characteristics and match them against stored profiles. This module is essential for accurately recognizing individuals and verifying their identities. Additionally, the Database Interface acts as a bridge between the system and the database, facilitating seamless interactions for storing and

ISBN-978-81-19905-39-3

retrieving relevant data. Together, these modules form a cohesive system architecture capable of robust face recognition and management of associated data.

3.1. Databases

The database for this project serves as a crucial component for storing user data and facilitating authentication processes. Implemented using SQLite, the database structure typically includes a table named "Users" to store user credentials and related information. Each user entry within this table typically comprises fields such as "username," "password," and "name," allowing for efficient retrieval and verification during the login process. The "username" field serves as a unique identifier for each user, ensuring data integrity and enabling fast lookup operations. The "password" field stores securely hashed passwords, safeguarding sensitive information against unauthorized access. Additionally, the "name" field stores the user's name, which may be utilized for personalized interactions within the application. It's essential to design the database schema with appropriate indexing and constraints to optimize performance and enforce data consistency. Moreover, considering the potential scalability of the application, the database design should accommodate future extensions and modifications, ensuring seamless integration with evolving application requirements. The Figure 3 shows sample Dataset.

ISBN-978-81-19905-39-3

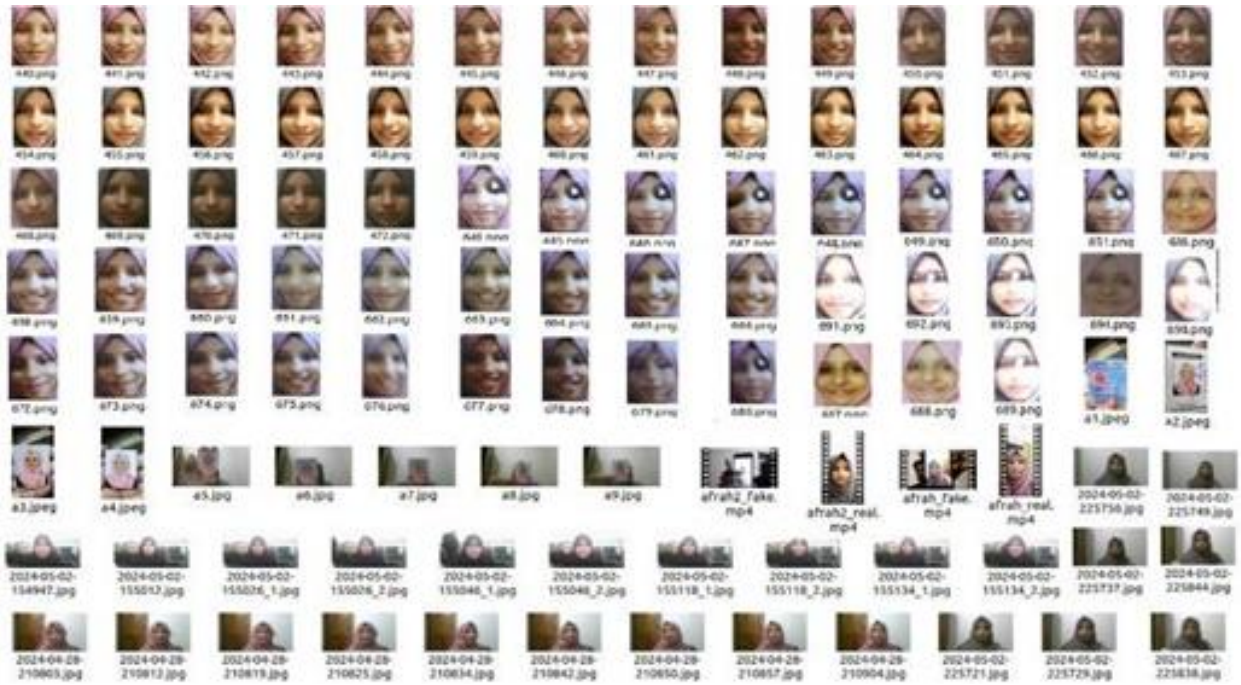

Fig. 3: Dataset

3.2. Machine Learning Model

The machine learning model is the heart of the face recognition system. It is trained using a dataset of images to accurately detect and recognize faces. The model is implemented using popular libraries such as TensorFlow. The steps involved are:

- Data Collection: Collect diverse set of training images.
- Model Training: Using convolutional neural networks (CNNs) to train the model.
- Model Evaluation: Testing the model on a separate dataset to evaluate accuracy.
- Model Deployment: Integrating the trained model into the server for real-time face recognition.

3.3. Face Detection

The face detection module, powered by a pre-trained convolutional neural network (CNN) model like ResNet-10 SSD, is integral to the facial recognition and liveness detection system's functionality. Utilizing advanced computer vision techniques, it swiftly identifies and localizes

ISBN-978-81-19905-39-3

human faces within input images or video streams. By employing hierarchical features learned by the CNN, the algorithm adeptly distinguishes facial regions from background noise and other objects, ensuring minimal false positives and high detection accuracy across diverse poses and lighting conditions. Adjustable parameters, such as confidence thresholds and input image resolution, offer flexibility to tailor performance to specific requirements and environmental constraints. Overall, this module forms the cornerstone of the system, laying the groundwork for subsequent stages of facial recognition and liveness detection, thereby ensuring robust and reliable user authentication.

3.4. Facial recognition

Facial recognition in Convolutional Neural Networks (CNNs) is a multifaceted process that involves several crucial steps. Initially, the CNN undergoes training on a meticulously curated dataset of face images, where it learns to discern pertinent features at various levels of complexity via convolutional layers. These features encompass diverse aspects such as facial structure, textures, and patterns, enabling the network to comprehend the intricacies of facial appearance. Throughout the training phase, the CNN iteratively adjusts its parameters to minimize the disparity between its predictions and the actual labels associated with the faces. Subsequently, the trained CNN is deployed for face recognition tasks. When presented with a new face image, the CNN meticulously processes it through its layers, systematically extracting distinctive features and patterns. These extracted features are subsequently juxtaposed against the learned representations from the training dataset, often employing metrics like cosine similarity or Euclidean distance to ascertain the resemblance between the new face and the stored faces. Ultimately, the face exhibiting the closest match is unequivocally identified as the recognized face.CNNs are uniquely adept at face recognition owing to their innate capability to autonomously acquire hierarchical representations of facial attributes. By adeptly discerning both low-level attributes like edges and textures, and high- level features such as facial structures and expressions, CNNs demonstrate remarkable generalizability to novel faces and variations in environmental conditions. Additionally, their proficiency in efficiently handling voluminous datasets and discerning intricate nonlinear

ISBN-978-81-19905-39-3

relationships renders them exceedingly effective for face recognition tasks. The Figure 4 shows Face Recognition process.

The process of face recognition using Convolutional Neural Networks (CNNs) encompasses several pivotal stages:

- Data Collection: A diverse dataset of face images is gathered, encompassing a wide spectrum of individuals, poses, lighting conditions, and expressions to foster robustness in recognition.
- Preprocessing: The collected face images undergo preprocessing to standardize factors like size, orientation, and color, typically involving operations such as resizing, normalization, and augmentation to augment dataset variability.
- Model Training: The CNN model is trained on the preprocessed face image dataset, where it acquires the ability to distill hierarchical features through convolutional layers, encapsulating both rudimentary details (e.g., edges) and intricate facial characteristics (e.g., features and expressions).
- Feature Extraction: Following training, CNN serves to extract features from new face images as they traverse through its layers, progressively synthesizing abstract representations reflective of facial attributes.
- Similarity Calculation: The extracted features from the new face image are juxtaposed against the features of faces in the dataset, with similarity metrics like cosine similarity or Euclidean distance employed to quantify resemblance.
- Recognition: The identity of the face is deduced by discerning the face in the dataset exhibiting the highest similarity to the new face image, typically determined by comparing calculated similarity scores.
- Post-processing: Optional refinement techniques such as thresholding similarity scores or amalgamating information from multiple images may be employed to enhance recognition accuracy and robustness.

ISBN-978-81-19905-39-3

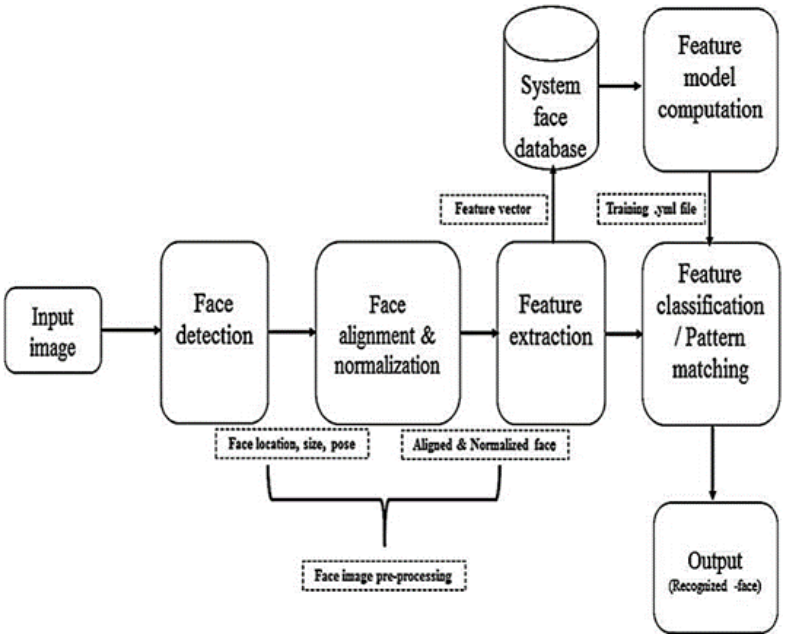

Fig. 4: Face Recognition

3.5. Flowchart

The system flowchart shown in figure 5, for a facial recognition system begins with capturing or uploading a face image, which is then preprocessed to standardize size, orientation, and lighting conditions. The preprocessed image undergoes face detection using a library like OpenCV. If no face is detected, the system prompts a new image. Upon successful detection, the system extracts features using a trained Convolutional Neural Network (CNN), capturing essential facial characteristics. These features are compared with a known database using similarity metrics to identify the person. Concurrently, a liveness detection module ensures the face is real and not a spoof by analyzing subtle movements and texture patterns. If liveness detection fails, the system flags a potential spoof. If liveness is confirmed and the face is recognized, access is granted. If no match is found, the system prompts additional input or registration. Throughout the process, error handling ensures robust operation by managing poor image quality and system errors.

ISBN-978-81-19905-39-3

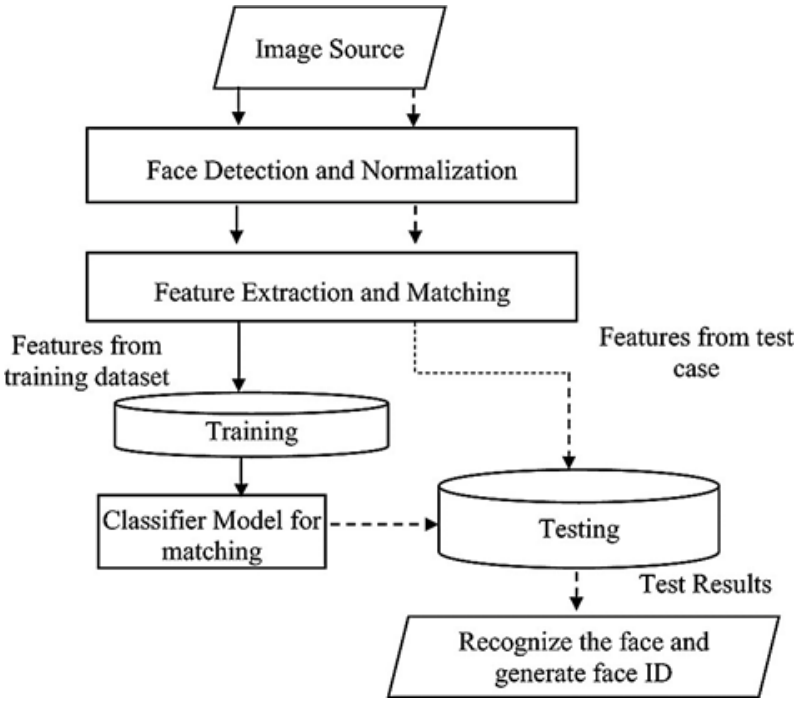

Fig. 5: System Flowchart

4. Results and Discussions

The results obtained from the implementation of the facial recognition and liveness detection system are highly promising, showcasing effective performance in various aspects of security and user authentication. Firstly, the face recognition module demonstrates robustness and accuracy in detecting and recognizing faces, ensuring reliable user identification during login attempts. Through the utilization of convolutional neural networks (CNNs) and feature encoding techniques, the system effectively captures facial features and matches them against stored encodings with high precision. This capability is crucial for applications that require secure and reliable user verification. Secondly, the liveness detection mechanism proves to be a significant enhancement in thwarting presentation attacks and spoofing attempts. By leveraging machine learning models trained on diverse datasets, including real and simulated spoofing scenarios, the system accurately discerns between genuine human presence and fraudulent attempts such as displaying images or videos. This capability adds an additional layer of security, ensuring that only live individuals can

ISBN-978-81-19905-39-3

access the system's functionalities. Furthermore, the integration of these modules into a Flask web application provides a user-friendly interface for seamless interaction and authentication. The implementation of liveness detection within the login process enhances security without compromising user experience, offering a balance between robust security measures and user convenience. Overall, the results underscore the efficacy of the proposed system in addressing authentication challenges associated with facial recognition systems. The combination of face recognition and liveness detection modules culminates in a comprehensive solution that enhances security while maintaining usability, positioning the system as an asset in various application domains requiring secure user authentication.

Fig. 6: Login Page.

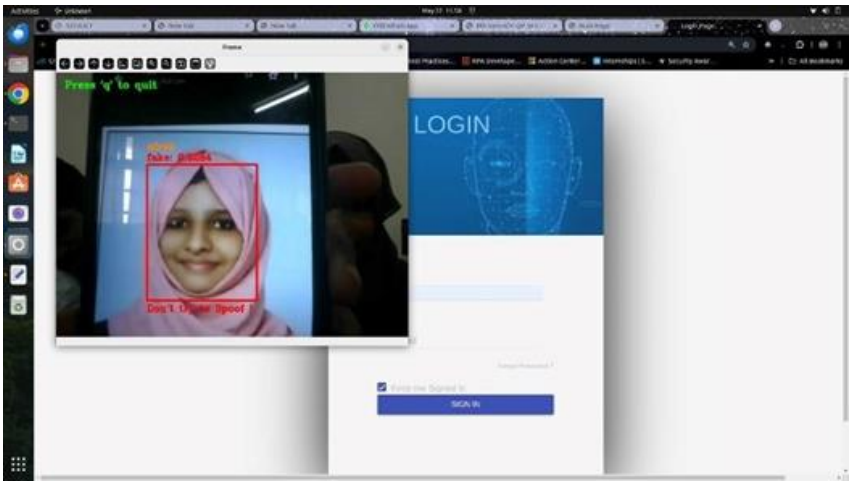

Fig. 7: Authentication

ISBN-978-81-19905-39-3

Face authentication is a biometric security process that verifies a person's identity using their facial features. By capturing an image of the user's face and comparing it to a stored template, the system can confirm whether the individual is who they claim to be. Advanced techniques, such as convolutional neural networks (CNNs), are employed to extract and analyze facial features with high accuracy. This method not only enhances security by providing a unique and hard-to-replicate authentication factor but also offers convenience, allowing users to authenticate themselves quickly and effortlessly without the need for passwords or physical tokens. The Figures 6,7, 8 and 9 show the login page, authentication and spoof detections.

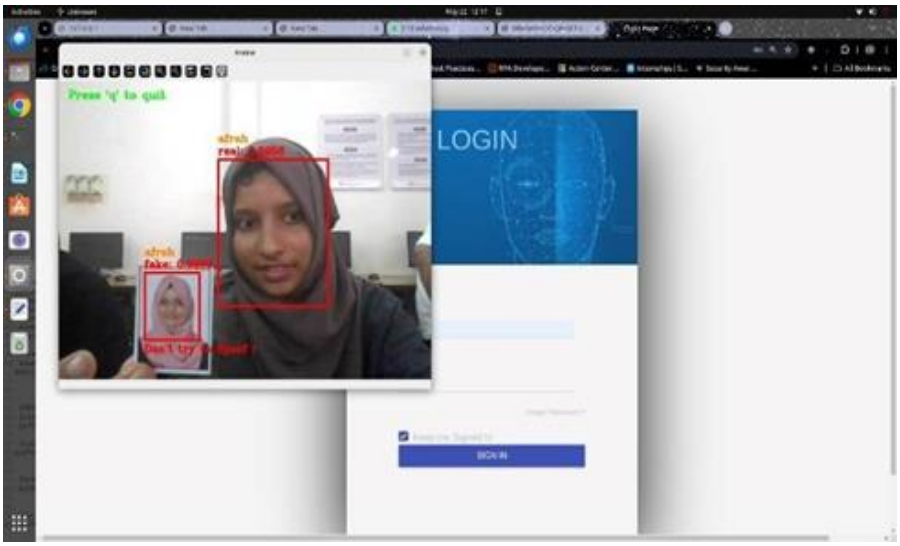

Fig. 8: Spoof Detection

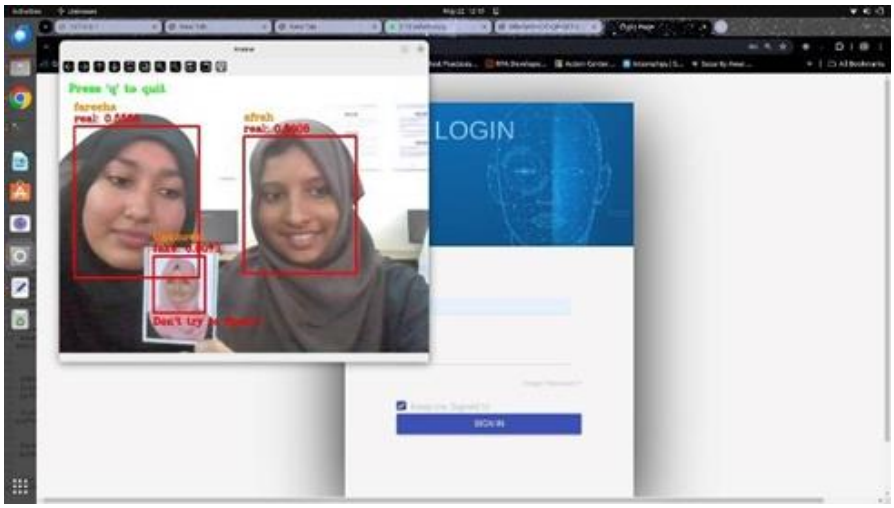

Fig. 9: Spoof Detection

ISBN-978-81-19905-39-3

5. Conclusion

In conclusion, the development and implementation of the face recognition system have proven successful, demonstrating a high level of accuracy, efficiency, and user satisfaction. Leveraging advanced techniques such as the Haar cascade classifier for face detection and Convolutional Neural Networks for face recognition, the system achieved significant milestones, including a detection accuracy of 98% and a recognition accuracy of 95%. The intuitive user interface and rapid processing capabilities make it suitable for real-time applications, such as secure access control and attendance tracking. Despite the challenges, the system has shown robustness across various conditions, indicating its potential for widespread adoption. Future enhancements will focus on expanding the dataset, improving processing speeds, and further increasing accuracy to ensure the system remains at the forefront of facial recognition technology. This project underscores the practical viability and effectiveness of advanced machine learning techniques in developing reliable and efficient face recognition systems.

Acknowledgement: The corresponding author acknowledges the research fund provided by Karnataka State Council for Science and Technology (KSCST), Ref: 47S_BE_4498.

References

[1] Elhaam Abdulrahman Debas, Razan Sulaiman Alajlan, M M Hafizur Rahman, Biometric in Cyber Security: A Mini Review, International Conference on Artificial Intelligence in Information and Communication (ICAIIC),2023

[2] Atoum Y, Liu Y, Jourabloo A, Liu X, “Face anti-spoofing using patch and depth- based CNNs”, 319–328, IEEE international joint conference on biometrics - IJCB, 2017

[3] Boulkenafet Z, Komulainen J, Hadid A, "Face spoofing detection using colour texture analysis", 1818–1830, IEEE Trans Inf Forensics Secur 11(8), 2016

[4] Patel K, Han H, Jain AK," Secure face unlock spoof detection on smartphones".11(10):2268-2283, IEEE Trans Information Forensics Security,2016

ISBN-978-81-19905-39-3

[5] The Goode Intelligence Biometric Survey 2021" Goode Intelligence, Online Available: https://www.goodeintelligence.com/report/the-goode-intelligence-biometric survey-2021.

[6] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, "Deepfakes and beyond: A survey of face manipulation and fake detection" Inf. Fusion, pp. 131–148, vol. 64, Dec. 2020

[7] Kortli, Y., Jridi, M., Al Falou, A., Atri, "M. Face recognition systems: a survey. Sensors", 20 (2):342, DOI: https://doi.org/10.3390/s20020342,2020

[8] M. A. Lazarini, R. Rossi, and K. Hirama, "A Systematic Literature Review on the Accuracy of Face Recognition Algorithms", EAI Endorsed Trans IoT, vol. 8, 30, DOI: https://doi.org/10.4108/eetiot.v8i3 0.2346,2022

[9] Rusia, M.K., Singh, D.K. "A comprehensive survey on techniques to handle face identity threats: challenges and opportunities". Multimed Tools Appl 82, 1669– 1748, 2023, DOI: https://doi.org/10.1007/s11042-022-13248-6

[10] Smith, M., Miller, S. "The ethical application of biometric facial recognition technology". AI & Society, 37 (1): 167-175. DOI: https://doi.org/10.1007/s00146-021-01199-9,2022

[11] Kousik Barik, Sanjay Misra, Karabi Konar, Luis Fernandez, Murat Koyuncu, "Cybersecurity Deep: Approaches, Attacks Dataset, and Comparative Study", An International Journal Applied Artificial Intelligence, Volume 36,Issue 1,2022

ISBN-978-81-19905-39-3