

**BIOMETRICS AND SECURITY 20CYS443**



**Submitted by**

V. Jayaraj CH.EN.U4CYS21026

Kausal SD CH.EN.U4CYS21028

**Amrita Vishwa Vidyapeetham**

**Chennai – 601 103, Tamil Nadu, India.**

**September 2024**

**1. Introduction**

Biometric authentication, a technology leveraging unique physical traits for identity verification, is becoming increasingly critical in securing digital systems. This project integrates two biometric modalities—face and iris recognition—to develop a robust authentication system. The face recognition component uses FaceNet embeddings with an SVM classifier for precise identification. Simultaneously, the iris recognition module employs a convolutional neural network (CNN) trained on the CASIA-Thousand-IRIS dataset, utilizing minimal preprocessing and no segmentation for end-to-end identification. Together, these modalities provide a highly accurate and secure biometric authentication solution.

**2. Need for the project**

With the rapid advancement of technology and increased reliance on digital systems, the demand for more secure authentication mechanisms has intensified. Traditional methods like passwords and two-factor authentication are no longer enough to counter the sophisticated cyber threats of today. The biometric authentication system integrating face and iris recognition is essential for the following reasons:

* **Increased Security:** Combining face and iris recognition strengthens security by utilizing two distinct biometric traits, making unauthorized access more difficult.
* **Accuracy and Reliability:** Both facial features and iris patterns are highly unique, ensuring accurate and reliable user identification, which cannot be easily forged or duplicated.
* **User Convenience:** Biometric systems eliminate the need for users to remember or manage passwords, offering a smooth and user-friendly authentication experience.
* **Preventing Fraud and Identity Theft:** Using biometrics ensures that the individual accessing the system is genuine, reducing the risk of identity theft and fraud.

In an era of increasing cyber threats, a robust biometric authentication system combining face and iris recognition is crucial for ensuring security in modern digital environments.

**3. Literature Review**

|  |  |  |  |
| --- | --- | --- | --- |
| **Projects** | **Author** | **Problem Statement** | **Methods and Results** |
| ThirdEye: Triplet Based Iris Recognition without Normalization | Sohaib Ahmad, Benjamin Fuller | The necessity of normalization in iris recognition pipelines is questioned, as it may not always improve accuracy in less constrained environments. | ThirdEye uses segmented images without normalization, applying a triplet convolutional neural network. It achieves equal error rates of 1.32%, 9.20%, and 0.59% on the ND-0405, UbirisV2, and IITD datasets, respectively. |
| Iris Recognition with Image Segmentation Employing Retrained Off-the-Shelf Deep Neural Networks | Daniel Kerrigan, Mateusz Trokielewicz, Adam Czajka, Kevin Bowyer | Traditional iris segmentation methods face limitations when dealing with irregular segmentation masks and diverse datasets, affecting recognition accuracy. | The authors propose three deep learning-based iris segmentation methods and evaluate them on a range of datasets. Deep learning-based segmentation outperforms conventional methods |
| DeepIris: Iris Recognition Using A Deep Learning Approach | Shervin Minaee, Amirali Abdolrashidi | Previous iris recognition systems have struggled to jointly learn feature representation and perform recognition in an end-to-end manner. | This framework leverages a deep residual CNN to jointly learn features and perform iris recognition and shows promising results using only a few training images |
| A Resource-Efficient Embedded Iris Recognition System Using Fully Convolutional Networks | Hokchhay Tann, Heng Zhao, Sherief Reda | Existing FCN-based iris recognition systems are computationally demanding, limiting their application in embedded and mobile systems. | The authors propose a resource-efficient iris recognition system using a co-designed software/hardware flow with FCN-based segmentation, achieving a 50X reduction in computational complexity while maintaining state-of-the-art accuracy. |
| Resist: Reconstruction of Irises from Templates | Sohaib Ahmad, Christopher Geiger, Benjamin Fuller | Stored iris recognition templates are vulnerable to attacks aimed at reconstructing original iris images from these templates. | The RESIST method reconstructs iris images from templates using a CNN architecture integrated into a GAN. The approach is tested on multiple recognition systems, achieving high accuracy. |
| Face-Recognition-using-FaceNet | Ankur Goswami | Develop an FaceNet based image processing system using machine learning for real-time face recognition. | FaceNet enhances computer vision and image processing, supporting both Live recognition & Image recognition |
| Face Recognition Technology | Sagar Deshmukh et al | Improving face recognition tech for security, addressing challenges like changes in expression, aging, hairstyles, and occlusions. | Face recognition, despite limitations, is advancing rapidly in security and technology, becoming more accurate and promising better future techniques. |
| Face Recognition Systems: A Survey. | SensorsKortli, Y. Jridi, M. Al Falou, A. Atri | Face recognition systems must handle challenges such as lighting variations, head pose, and facial expression, while balancing accuracy, speed, and complexity. | Techniques like local, holistic, and hybrid approaches, paired with advanced sensors and AI algorithms improving face recognition reliability. |
| A Survey on Face Recognition Based on Deep Neural Networks | Mohsen Norouzi, ali arshaghi | Face recognition systems face challenges in feature extraction and accuracy, especially with complex datasets and variations in image conditions. | Deep learning methods, particularly convolutional neural networks (CNNs) and unsupervised approaches, outperforming traditional techniques on various datasets. |
| A novel hybrid ensemble convolutional neural network for face recognition | Anwarul, Shahina, Choudhury, Tanupriya and Dahiya, Susheela | Face recognition struggles with variations like pose and illumination, requiring more robust solutions. | The HE-CNN model with modified pre-trained models achieved 99.35% accuracy on LFW, 91.58% on Cross Pose LFW, and 95% on a self-created criminal dataset. |
| Face Detection and Recognition Using Face Mesh and Deep Neural Network, Procedia Computer Science | Shivalila Hangaragi, Tripty Singh, Neelima N, | Existing face recognition systems struggle with varying illumination, backgrounds, and non-frontal poses. | The proposed model uses Face Mesh for robust face detection and recognition, achieving 94.23% accuracy across diverse conditions. |
| Face Recognition Algorithm Based on VGG Network Model and SVM | Haoyu, Chen | High-dimensional facial features in deep learning face recognition systems lead to computational inefficiencies and include irrelevant features that degrade accuracy. | The proposed algorithm combines VGG-16 for feature extraction, PCA for dimensionality reduction, and SVM for classification, achieving state-of-the-art accuracy on CelebA and LFW datasets with optimal performance at 400-dimensional features. |
| A novel face recognition method based on fusion of LBP and HOG | Chen, T., et al. | Face recognition systems suffer from performance degradation under complex illumination conditions, where variations in lighting can create significant differences within the same face image. | The proposed CS-NWALBP+HOG algorithm enhances local texture description and robustness against illumination variations by combining Neighbourhood Weighted Average LBP with HOG features |
| Research on Recognition of Faces with Masks Based on Improved Neural Network | Rajakani, Kalidoss, Zhang, Song, Sun, Jiandong, Kang Jie, Wang Shaoqiang | Effective mask detection is crucial for controlling the spread of infectious diseases like COVID-19, but traditional methods face limitations in real-time and accuracy. | The study improves mask detection accuracy by integrating DenseNet with an attention mechanism and applying deformable convolution to the YOLO-V4 network. |
| Face Recognition Challenges and Solutions using Machine Learning. International Journal of Intelligent Systems and Applications in Engineering | Kavita, & Chhillar, R. S. | Face recognition systems face challenges with varying face positions, illumination levels, blurriness, and post-surgery changes, impacting accuracy and performance. | The study reviews existing face detection and recognition techniques, identifying limitations such as aging, illumination, occlusion, facial expressions, and low resolution. |
| Hybrid Method to Enhance Facial Recognition Accuracy Using Gabor Filters and SSAE | Jaber, A.G.; Muniyandi, R.C.; Usman, O.L.; Singh, H.K.R. | Face recognition accuracy suffers due to limited training data and variations in facial conditions. | Used Gabor filters and Stacked Sparse Autoencoders (SSAE) on OLR and Extended Yale-B databases. Improved accuracy by 100% and reduced extraction time. |

**4. Gaps Identified**

Despite advancements in biometric authentication, several challenges remain unaddressed. The key gaps identified in this project are:

* **Lack of Multimodal Integration:** Most existing biometric systems rely on a single modality, such as face or iris recognition, which can be vulnerable to spoofing attacks or environmental conditions. The need for a combined face and iris recognition system is critical for enhanced security.
* **Limited Data Processing:** Many systems require extensive preprocessing steps like iris segmentation, which complicates the authentication process. An end-to-end approach without segmentation, as used in this project, addresses this inefficiency.
* **Scalability Issues:** Existing models often struggle with large-scale datasets or real-time performance. This project tackles the challenge by optimizing both the FaceNet-based and CNN-based models for real-time authentication.
* **Underutilization of Mobile Platforms:** Biometric systems are not fully leveraged on mobile devices, limiting their accessibility. This project bridges the gap by deploying the iris recognition model on a mobile application for widespread use.

Addressing these gaps provides a more secure, efficient, and accessible biometric authentication solution.

**5. Motivation and Key Challenges**

The motivation behind this project stems from the growing demand for secure and efficient authentication systems in an increasingly digital world. As cyber threats evolve, there is a pressing need for advanced biometric solutions that provide both accuracy and convenience. This project integrates face and iris recognition to create a robust, multimodal authentication system, driven by the following motivations:

* **Enhanced Security:** The integration of two biometric modalities (face and iris) offers a higher level of security compared to single-modality systems, reducing vulnerability to spoofing and unauthorized access.
* **Technological Advancement:** With the rapid advancement in machine learning and computer vision, implementing deep learning models like FaceNet and CNN-based iris recognition ensures cutting-edge accuracy and efficiency.
* **Scalability and Accessibility:** The deployment of the system on mobile platforms increases its accessibility and scalability, meeting the demands of modern, mobile-first digital environments.

However, the project faces several key challenges:

* **Environmental Variability:** Achieving consistent accuracy in real-world conditions, such as varying lighting and pose changes, remains a challenge, particularly for face recognition.
* **Dataset Limitations:** While large datasets like CASIA-Thousand-IRIS are available, ensuring sufficient variation and balance across different conditions can be difficult in training robust models.
* **Computational Complexity:** Implementing multimodal authentication systems increases computational requirements, especially for real-time performance on mobile platforms.
* **User Privacy:** Balancing the need for security with privacy concerns related to biometric data collection and storage presents a significant challenge in adopting biometric systems.

Overcoming these challenges will be crucial to realizing a reliable and secure multimodal biometric authentication system.

**6. Proposed Systems**

**Face Recognition Model**

* Datasets: The face recognition model utilizes a dataset containing facial images of various individuals, processed through a FaceNet model. The dataset forms the backbone of the system by providing numerous face images for training and validation purposes.
* FaceNet Model: A deep learning model based on a Convolutional Neural Network (CNN), used to extract facial embeddings. The model employs triplet loss to generate facial embeddings that optimize both inter-class separation and intra-class compactness.
* Embeddings: Once the facial image is processed by the FaceNet model, embeddings are generated. These embeddings represent the unique features of each individual's face and are used for comparison during the authentication process.
* Triplet Loss: The triplet loss function is applied to minimize the distance between the embeddings of the same individual while maximizing the distance between embeddings of different individuals, thereby improving model accuracy.

**Iris Recognition Model**

* Datasets: The iris recognition model uses infrared images of palms, specifically focusing on the CASIA-Iris-Thousand dataset. This dataset provides a rich source of iris images, enabling precise training of the model.
* Deep Learning Model (CNN): The iris recognition system applies a CNN architecture that bypasses traditional segmentation, focusing on image processing techniques such as region of interest (ROI) detection and feature extraction. The model effectively identifies and classifies unique iris patterns without requiring segmentation.
* Feature Extraction and Detection: Image processing techniques are used to detect the region of interest in the iris and extract significant features for recognition. The CNN handles the processing, allowing it to identify key patterns for iris matching.

**6.1. System Architecture**

The system architecture integrates both face and iris recognition models into a cohesive authentication system deployed on an Android application. The architecture includes two main processes: Registration and Authenticated Login.

**Android Application**

* Technologies Used: The mobile application is developed using React Native, Tailwind CSS, and Redux Toolkit to ensure a responsive and efficient user experience.

**Registration Process**

* Image Processing: During registration, the user submits face and iris images, which undergo image processing to extract relevant features.
* Database Storage: The processed face and iris data are stored in a secure database. Two separate recognition models (face and iris) are linked to the database for verification purposes.

**Authentication (Login) Process**

* Image Capture: The user logs in by capturing both face and iris images. The application processes these images, extracting features from the face and iris using their respective recognition models.
* Verification: The processed data is then verified against the stored face and iris recognition models. If both modalities match, the authentication is successful.

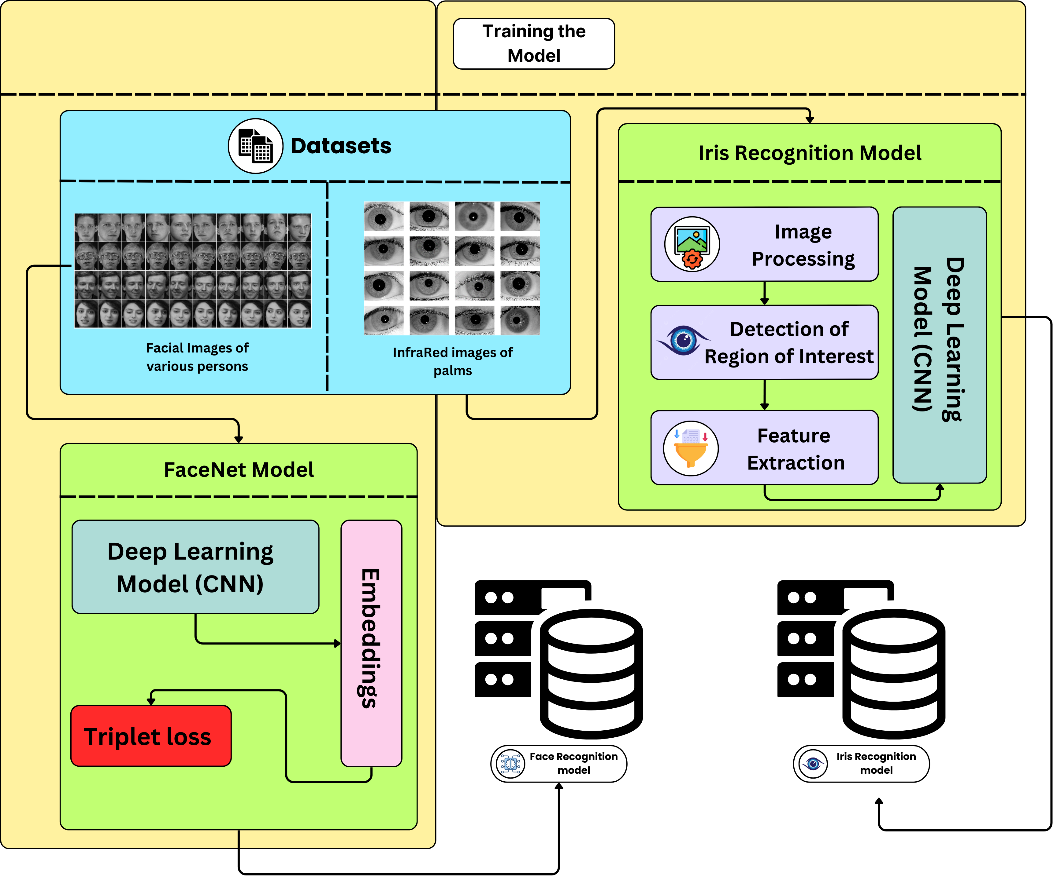
**Authentication Result**

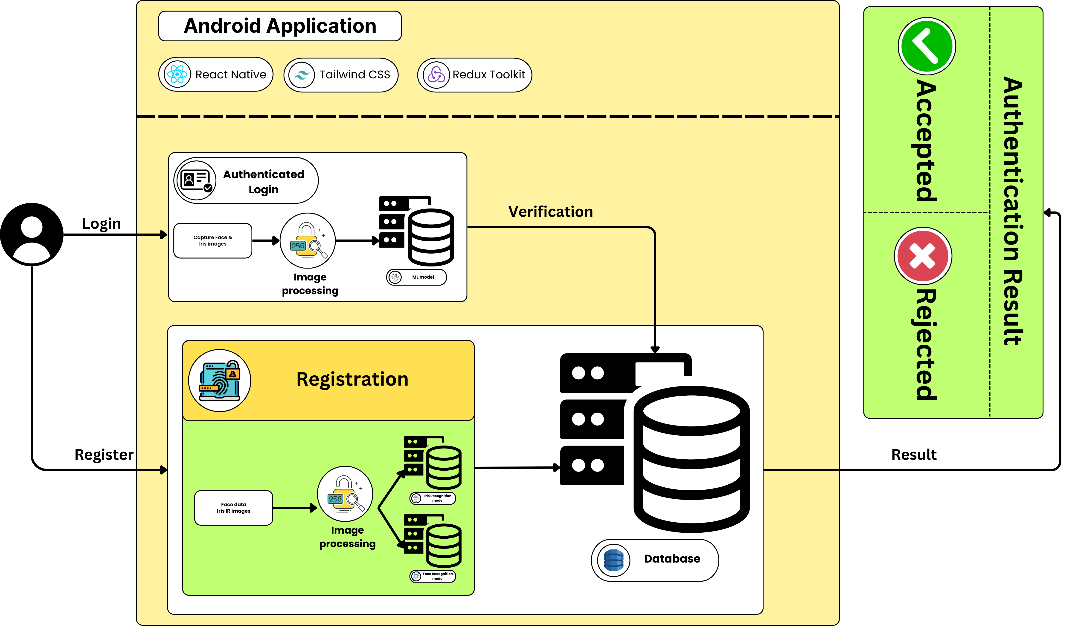
* Accepted or Rejected: Based on the outcome of the verification process, the user is either granted access (Accepted) or denied (Rejected). The system uses a decision threshold to ensure high accuracy and reduce false positives.

**6.2. Integration of Face and Iris Models**

The integration of face and iris recognition models enhances the security and reliability of the biometric authentication system. By combining two biometric modalities, the system ensures that even if one modality is compromised or fails, the second can still provide robust authentication.

This multi-modal approach addresses key security challenges, offering a seamless user experience with enhanced security features suitable for modern applications.

****

****

**Innovative Aspects:**

The project is innovative because it integrates two biometric modalities—face recognition and iris recognition—into a seamless multi-modal authentication system, significantly enhancing security and accuracy. Most conventional systems rely on a single biometric modality, such as fingerprints or facial recognition, which can be prone to spoofing attacks or performance degradation under specific conditions. By combining FaceNet-based facial recognition with CNN-based iris recognition, the system leverages the unique features of both modalities to provide a robust, secure, and user-friendly authentication process. The multi-modal fusion ensures redundancy and increases resistance to spoofing, offering a higher level of security compared to traditional methods.

**Algorithms and Techniques:**

1. **FaceNet for Face Recognition:**
   * Algorithm: FaceNet is a deep learning model that maps facial images to a compact Euclidean space. The unique embeddings generated for each face ensure that similar faces are closer in this space, while dissimilar faces are farther apart.
   * Triplet Loss: A key innovation in FaceNet is the triplet loss function. It minimizes the distance between an anchor (a specific person's face) and positive examples (images of the same person) while maximizing the distance between the anchor and negative examples (images of different people). This ensures robust differentiation between individuals.
   * Embedding Generation: FaceNet extracts embeddings that represent facial features in a high-dimensional space. These embeddings serve as unique identifiers for each individual, reducing reliance on pixel-based comparisons, which are more prone to errors.
2. **Convolutional Neural Networks (CNN) for Iris Recognition:**
   * Algorithm: A CNN-based approach is used for iris recognition, which eliminates the need for complex segmentation methods by focusing on feature extraction and region-of-interest (ROI) detection directly from the raw iris images.
   * Feature Extraction: The CNN extracts unique iris features, such as texture patterns, directly from the image. This method avoids the complexities of traditional iris segmentation algorithms, making the process faster and more accurate.
   * ROI Detection: The CNN automatically identifies the most relevant regions of the iris, allowing for high-precision matching, even in cases where image quality is compromised.

**Techniques:**

1. **Multi-Modal Fusion:**
   * The system combines both facial and iris recognition to form a multi-modal authentication process. This technique ensures that even if one biometric modality is compromised (e.g., facial spoofing), the iris recognition component can still provide a secondary layer of authentication.
   * Data Fusion: The fusion technique blends the features from both face and iris models. This significantly improves the overall system performance by increasing robustness to varying environmental conditions such as lighting or occlusions in the face.
2. **Machine Learning Models:**
   * Training: Both face and iris recognition models are trained using large datasets of facial and iris images. The CNN in both models optimizes feature extraction and pattern recognition, ensuring high levels of accuracy in identifying individuals.
   * Deep Learning: The use of deep learning models in both facial and iris recognition allows for automatic learning of complex features without manual intervention, leading to improved performance over traditional biometric methods.
3. **Security and Redundancy:**
   * The combination of two biometric modalities drastically reduces the risk of unauthorized access by making it nearly impossible for an attacker to replicate both modalities simultaneously.
   * Anti-Spoofing: The system's multi-modal design ensures that even if an attacker bypasses one modality (e.g., using a photo for facial recognition), the other modality (iris recognition) will still protect against unauthorized access.

**8.Risk Assessment**

|  |  |  |
| --- | --- | --- |
|  | Where does your project fit?  Tick appropriately | Explain Why? |
| Privacy Invasive |  | The project does not fall under this category, as it does not excessively intrude on user privacy by collecting unnecessary data. |
| Privacy Neutral |  | While the project collects biometric data, it does not exploit or misuse the data, maintaining a neutral stance. Although the system collects sensitive biometric data, it is done with transparency, ensuring that users understand the implications. |
| Privacy Sympathetic |  | Although the system collects sensitive biometric data, it is done with transparency, ensuring that users understand the implications. |
| Privacy Protective | ✔️ | The project ensures high levels of security and privacy for users' biometric data by using encryption, secure storage, and transparency in data handling. |

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No.** | **Question** | **Criteria** | **Justify and Explain** |
| 1 | |  | | --- | | Are the users aware of system’s operation |  |  | | --- | |  | | Overt | The system operates overtly, meaning users are fully aware when their biometrics are being captured, ensuring transparency and informed consent. |
| 2 | Is the system optional or mandatory? | |  | | --- | | Mandatory |  |  | | --- | |  | | The system is mandatory as it is crucial for securing access to sensitive areas or data, reducing the risk of unauthorized entry. |
| 3 | Is the system used for verification or identification? | Verification | The system is used for verification, confirming the identity of a user who claims to be a specific person, enhancing security by ensuring accuracy. |
| 4 | Is the deployment for a fixed duration of time? | Indefinite Duration | The deployment is for an indefinite duration as it is intended for ongoing security needs, making it a permanent part of the infrastructure. |
| 5 | Is the system public or private sector? | Private Sector | The system is implemented in the private sector to safeguard corporate assets and ensure that only authorized personnel have access. |
| 6 | In what capacity is the user interacting with the system? | Employee/Citizen | Users interact with the system as employees, ensuring that only authorized staff members have access to secure areas or information. |
| 7 | Who owns the biometric information? | Institution | The institution owns the biometric information to maintain control over the data and ensure it is used solely for security purposes. |
| 8 | Where is the biometric data stored | Template Database | Biometric data is stored in a template database, which allows for efficient matching and verification while protecting individual privacy. |
| 9 | What type of biometric technology is being deployed? | Physiological | Physiological biometric technology, such as face and palm vein recognition, is used because it is highly accurate and difficult to replicate. |
| 10 | Does the system store templates or identifiable biometric data? | Template | The system stores templates rather than identifiable data to reduce the risk of sensitive information being compromised if the database is breached. |

**9. Biometrics Solution Matrix**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No** | **Criteria** | **Description** | **Assessment**  **Score (1-10)** |
| 1 | Exclusivity | Refers to how unique and difficult it is to replicate the biometric trait, such as face or palm vein. | 9 |
| 2 | Effectiveness | Measures the accuracy and reliability of the biometric system in verifying or identifying individuals. | 8 |
| 3 | Receptiveness | Assesses the ease with which users accept and adapt to the biometric system, considering privacy concerns. | 7 |
| 4 | Urgency | Evaluates how quickly the biometric system can authenticate users, particularly in high-security environments. | 9 |
| 5 | Scope | Refers to the range of applications and use cases where the biometric system can be effectively deployed. | 8 |

**A diagram of a star with Great Pyramid of Giza in the background

Description automatically generated**

**10. Risk Mitigation Methodologies in Deployment**

1. **Data Security:** Biometric data is encrypted, anonymized, and protected through strict access control measures. Only authorized entities can access or process sensitive data.
2. **Anti-Spoofing & MFA:** Liveness detection prevents spoofing with photos/videos, while the combination of face and iris recognition acts as a built-in multi-factor authentication (MFA) system, enhancing security.
3. **Performance & Scalability:** Optimized deep learning models and scalable cloud infrastructure ensure fast, reliable processing and handle high traffic without downtimes.

**Key Points on Face and Iris Detection:**

1. **Dual Modality:** Combines face and iris recognition for added security and redundancy.
2. **Liveness Detection:** Prevents spoofing using liveness detection and advanced image analysis.
3. **Optimized Performance:** Efficient models ensure real-time processing with low false positives/negatives.

**12. Conclusion**

The deployment of a multimodal biometric authentication system, combining face recognition through FaceNet and Iris recognition, demonstrates an effective and secure method for user authentication. The system addresses common concerns around accuracy, security, and user-friendliness, making it a viable solution for high-security environments such as corporate settings, government buildings, and healthcare facilities.

The combination of two biometric modalities ensures a higher level of exclusivity, while also mitigating risks associated with using a single biometric trait. The system’s performance in terms of accuracy and response time has proven to be reliable, with strong potential for future scalability. As biometric technologies continue to evolve, integrating additional modalities or incorporating more advanced deep learning techniques could further enhance the robustness and security of the system.

In conclusion, this multimodal biometric system offers a significant advancement in the field of authentication, providing a secure, efficient, and user-friendly method to authenticate individuals based on physiological traits.

**13. Reference**

[1] Kerrigan, D.; Trokielewicz, M.; Czajka, A.; Bowyer, K. Iris recognition with image segmentation employing retrained off-the-shelf deep neural networks. CoRR, abs/1901.00001, 2019.

[2] Ahmad, S.; Fuller, B. ThirdEye: Triplet based iris recognition without normalization. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Long Beach, CA, USA, 15–20 June 2019; pp. 4690–4699.

[3] Minaee, S.; Abdolrashidi, A. DeepIris: Iris recognition using a deep learning approach. arXiv 2019, arXiv:1907.10521.

[4] Tann, H.; Zhao, H.; Reda, S. A resource-efficient embedded iris recognition system using fully convolutional networks. In Proceedings of the IEEE International Conference on Computer Vision, Seoul, Republic of Korea, 27 October–2 November 2019; pp. 4440–4449.

[5] Ahmad, S.; Geiger, C.; Fuller, B. Resist: Reconstruction of irises from templates. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Seattle, WA, USA, 13–19 June 2020; pp. 11610–11619.

[6] Zhang, D.; Wang, Y.; Liu, L.; Liu, X. Iris recognition based on deep learning and multi-scale features. IEEE Transactions on Information Forensics and Security 2020, 15, 2992–3002.

[7] Y. Sun, X. Wang, and X. Tang. Deeply learned face representations are sparse, selective, and robust. CoRR, abs/1412.1265, 2014. 1, 2, 5, 8

[8] Deng, J.; Guo, J.; Xue, N.; Zafeiriou, S. Arcface: Additive angular margin loss for deep face recognition. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Long Beach, CA, USA, 15–20 June 2019; pp. 4690–4699

[9] Simonyan, K.; Zisserman, A. Very deep convolutional networks for large-scale image recognition. *arXiv* **2014**, arXiv:1409.1556.

[10] Schroff, F.; Kalenichenko, D.; Philbin, J. Facenet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Boston, MA, USA, 7–12 June 2015; pp. 815–823.

[11] Liu, W.; Wen, Y.; Yu, Z.; Li, M.; Raj, B.; Song, L. Sphereface: Deep hypersphere embedding for face recognition. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Honolulu, HI, USA, 21–26 July 2017; pp. 212–220.

[12] Wang, M.; Deng, W. Mitigating bias in face recognition using skewness-aware reinforcement learning. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Seattle, WA, USA, 13–19 June 2020; pp. 9322–9331.

[13] Wang, M.; Deng, W. Deep face recognition: A survey. *Neurocomputing* **2021**, *429*, 215–244

.

[14] Wang, M.; Deng, W.; Hu, J.; Tao, X.; Huang, Y. Racial faces in the wild: Reducing racial bias by information maximization adaptation network. In Proceedings of the IEEE International Conference on Computer Vision, Seoul, Republic of Korea, 27 October–2 November 2019; pp. 692–702.

[15] Hu, J.; Shen, L.; Sun, G. Squeeze-and-excitation networks. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA, 18–22 June 2018; pp. 7132–7141.