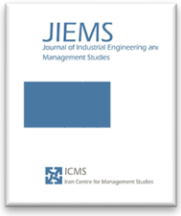
Vol. 11, No. 2, 2024, Pages 105_122

JIEMS
Journal of Industrial Engineering and Management Studies

journal homepage: www.jiems.icms.ac.ir



# Utilizing Biometric Authentication to Prevent Private Sharing of Physician Information for Prescription System Access

Ahrar Hosseini [1], Behrooz Khalil Loo [2], Amir Aghsami [3*]

[1] National Center for Health Insurance Research, Tehran, Iran.
[2] Department of Computer Science and Statistics, University of Rhode Island, Kingston, RI, USA.
[3] School of Industrial Engineering, K. N. Toosi University of Technology (KNTU), Tehran, Iran.

Received: Jul 2024-12/ Revised: Agu 2024-30/ Accepted: Apr 2024-20

**Abstract**

In the landscape of healthcare, ensuring the accuracy and security of prescription processes is crucial for maintaining patient safety and upholding ethical standards. This paper presents a novel biometric authentication framework designed to address the vulnerabilities in traditional authentication methods such as passwords and codes, which are prone to misuse. By integrating fingerprint and iris recognition, the proposed multi-modal system provides a robust solution to prevent unauthorized access to prescription data. This study collected biometric data from 600 doctors, comprising 600 fingerprint images and 1200 iris images, to rigorously evaluate the system's performance. Detailed information about the CNN architecture, including layers, activation functions, and loss functions, is provided. The model's effectiveness was measured using comprehensive metrics such as accuracy, precision, recall, and F1-Score, demonstrating a significant improvement over existing method. Furthermore, a statistical analysis was conducted to verify the reliability of the results, with comparisons drawn against baseline methods. The findings underscore the importance of enhancing biometric authentication systems and contribute to the development of secure and reliable identity verification solutions across the healthcare sector. This research not only bolsters the security of prescription processes but also reinforces the ethical principles guiding medical practice, offering a significant step forward in preventing fraud in healthcare systems.

**Keywords**: Biometric authentication, Fingerprint recognition, Iris recognition, Multi-modal authentication, Identity verification.

**Paper Type**: Original Research

## 1. Introduction

Prescription fraud represents a longstanding challenge in healthcare systems, necessitating a thorough understanding of its underlying causes and implications (Mantzana, Koumaditis, & Themistocleous, 2011). Previous research has extensively documented various forms of prescription fraud, including unauthorized refills, prescription forgery, and illegal diversion of controlled substances (Zafari & Ekin, 2019). Studies have also highlighted the significant financial costs associated with prescription fraud, estimating billions of dollars in losses annually for healthcare providers and insurers (Kumaraswamy, Markey, Barner, & Rascati, 2022). In addition to its economic impact, prescription fraud poses serious risks to patient safety and public health. Cases of fraudulent prescriptions often result in improper medication use, adverse drug interactions, and even patient harm or fatalities. Recognizing these consequences, researchers have explored different strategies for detecting and preventing prescription fraud, ranging from enhanced authentication measures to advanced data analytics and machine learning algorithms (Li et al., 2024; Mamoudan, Forouzanfar, Mohammadnazari, Aghsami, & Jolai, 2023). One area of focus in addressing prescription fraud involves improving the authentication systems used to verify the identity of prescribing physicians (Marino, Penedo, Penas, Carreira, & Gonzalez, 2006). Previous studies have evaluated the effectiveness of various authentication methods, including password-based systems, biometric authentication, and two-factor authentication (Al-Waisy, Qahwaji, Ipson, Al-Fahdawi, & Nagem, 2018; Jiang et al., 2020). While traditional methods such as password-based systems have proven susceptible to exploitation, recent advancements in biometric authentication, such as fingerprint recognition and iris scanning, offer promising solutions for enhancing the security and integrity of prescription processes. Moreover, researchers have investigated the role of technology, such as image processing techniques and artificial intelligence, in bolstering fraud detection capabilities in

*Corresponding Author: a.aghsami@ut.ac.ir

healthcare systems. The modus operandi of prescription fraud typically involves pharmacies exploiting loopholes in the authentication process to manipulate prescriptions. This manipulation may take various forms, ranging from unauthorized refills and alterations to dosage or medication type to the outright creation of fraudulent prescriptions (Matloob, Khan, ur Rahman, & Hussain, 2020). Such fraudulent activities not only pose significant risks to patient safety but also undermine the trust and integrity of the healthcare system as a whole. Recognizing the urgent need for more robust fraud detection measures, this paper advocates for a paradigm shift in doctor authentication towards image-based methods, specifically leveraging advanced image processing techniques, such as Convolutional Neural Networks (CNNs) (Mousapour Mamoudan, Ostadi, Pourkhodabakhsh, Fathollahi-Fard, & Soleimani, 2023). By harnessing the power of CNNs to analyze doctors' biometric features, such as fingerprints and iris patterns, healthcare systems can establish a more secure and reliable authentication process, thus enhancing fraud detection capabilities. The proposed image-based authentication approach offers several inherent advantages in the realm of fraud detection. By capturing and analyzing unique biometric characteristics, CNNs can accurately verify the identity of doctors, thereby significantly reducing the risk of fraudulent activities perpetrated by unauthorized individuals. Moreover, the adoption of image-based authentication not only enhances security but also reinforces the ethical principles governing medical practice, thus fostering a culture of accountability and integrity within the healthcare community. By addressing the vulnerabilities in current authentication systems and introducing innovative fraud detection mechanisms, this paper endeavors to fortify healthcare systems against the pervasive threat of prescription fraud, thereby safeguarding patient well-being and upholding the integrity of medical practice. This study presents a case focused on developing a robust biometric authentication system that utilizes fingerprint and iris biometric features (Vensila & Boyed Wesley, 2024). Biometric authentication systems are essential for ensuring secure access control and identity verification across various sectors, including healthcare (Lucia, Zhiwei, & Michele, 2023), inance, and law enforcement. By leveraging advancements in biometric technology, this research explores the effectiveness of a multi-modal approach to enhance the accuracy and reliability of identity verification processes. The study is grounded in the collection of biometric data from 600 doctors, including 600 fingerprint images and 1200 iris images, which forms the core of the evaluation framework. Through rigorous performance analysis using metrics such as accuracy, coverage, and F1-Score, this research aims to contribute valuable insights into the design and implementation of effective biometric authentication systems. The primary objective of this study is to develop and evaluate a robust biometric authentication system that utilizes fingerprint and iris biometric features for accurate and reliable identification of doctors. This research seeks to answer the following key questions: 1) Can a multi-modal approach, combining fingerprint and iris data, improve the accuracy and reliability of the authentication process compared to traditional methods? 2) How does this system perform under varying environmental conditions and with different data quality? and 3) Is the proposed system capable of minimizing both false positives and false negatives, thereby preventing unauthorized access to sensitive medical systems? By testing these hypotheses, this study aims to contribute to the advancement of biometric authentication systems in healthcare, enhancing security and trust in these systems. The study is structured into 5 sections. The second part will entail a review of the literature concerning the subject, while the third part will scrutinize the proposed methodology. In the fourth section, we will delve into the results obtained. Subsequently, in the fifth section, we will explore the implementation challenges and considerations, elucidating the benefits of Image-Based Authentication in Healthcare Systems and discussions pertaining to Future Directions and Recommendations.

## 2. Literature Review

Prescription fraud, an insidious phenomenon plaguing healthcare system worldwide, is a multifaceted issue with far-reaching implications. At its core, prescription fraud involves the illicit manipulation of medical prescriptions for personal gain, often at the expense of patient well-being and the integrity of healthcare practices. This pervasive problem undermines the fundamental principles of medical ethics and erodes the trust that patients place in their healthcare providers. Efficient patient identification in medical settings, especially during emergencies, is vital for prompt care delivery. Biometric authentication systems offer a solution by accurately identifying individuals based on unique biometric features. Kurgan, Cios, and Dick (2006) presented a real-time decision support system focusing on fingerprint data analysis employing a rule-based technique, addressing computational complexity and memory constraints. Díaz-Palacios, Romo-Aledo, and Chinaei (2013) proposed a biometric system accessing centralized health records, ensuring patient privacy in emergencies. Utilizing biometric terminals with mobile phone technology, their system securely transmits patient fingerprints to central databases, enabling health record retrieval while preserving privacy in pre-hospital settings. Bhattasali, Saeed, Chaki, and Chaki (2014) proposed a multifaceted biometric authentication approach to mitigate health data misuse in heterogeneous cloud environments, incorporating keystroke dynamics and facial recognition to improve authentication accuracy. Mamat, Rasam, Adnan, and Abdullah (2014) introduced a hybrid biometric authentication system for healthcare, verifying

unconscious patients through fingerprint, facial, or iris scans, while conscious patients can present national identification cards. proposed a biometric system accessing centralized health records, ensuring patient privacy in emergencies. Utilizing biometric terminals with mobile phone technology, their system securely transmits patient fingerprints to central databases, enabling health record retrieval while preserving privacy in pre-hospital settings. Additionally, a novel multimodal biometric identification system introduced in 2017 integrated facial biometrics, left iris, and right iris utilizing deep learning techniques. This system employed a deep belief network architecture for facial feature definition and a combination of convolutional neural network and softmax classifier for iris recognition, extracting distinctive features from iris images (Al-Waisy, Qahwaji, Ipson, & Al-Fahdawi, 2017). Aparna and Kishore (2019) explored the integration of biometric authentication systems into electronic health records, aiming to enhance security and privacy. One study investigated combining fingerprint and facial recognition biometrics for authentication, employing fingerprint biometrics for authentication, encryption for confidentiality, and reversible watermarking for data integrity. Shakil, Zareen, Alam, and Jabin (2020) introduced a cloud-based healthcare data management system ensuring electronic medical data security through signature scanning-based authentication. Utilizing neural networks for data analysis, their results exhibited a substantial enhancement in test speed (9 times), with an error rate of 0.12, sensitivity of 0.98, and specificity of 0.95. In 2022, Sarier proposed a model for hybrid biometric authentication and patient privacy protection schemes in healthcare systems using blockchain technology, demonstrating its potential to establish a natural barrier against data security issues. Mason et al. (2020) innovated by integrating eye biometrics into healthcare systems for robust patient identification. Their method combines eye-related biometrics with electronic indices within health information systems, enhancing patient identification accuracy. Meanwhile, Heidari and Chalechale (2022) proposed a multimodal biometric approach to bolster authentication in healthcare settings and combat fraud. Leveraging deep learning techniques on a dataset comprising 1090 samples, they authenticated individuals based on hand biometric features, including nails, fingerprints, and specific finger characteristics. Alghamdi, Angelov, and Alvaro (2022) employed deep learning and various neural networks to analyze biometric data associated with finger joints and nails for individual identification. Their approach integrates automatic person recognition through component localization, detection, and segmentation, along with similarity matching between segmented images. Additionally, they introduced a multimodal biometric authentication system to enhance data security, addressing the limitations of unimodal authentication approaches. Srivastava and Sharma (2022) proposed a hybrid framework combining principal component analysis and linear binary pattern to authenticate individuals using face and palm print biometrics, generating a unique score for authentication. Alaa et al. (2018) proposed a real-time multimodal biometric system leveraging deep learning representations for both left and right iris images. Named IrisConvNet, the system employs a combination of CNN and Softmax classifier to extract discriminative features without domain knowledge. Training strategies including back-propagation and mini-batch AdaGrad optimization are utilized, alongside dropout methods and data augmentation. Performance evaluation on public datasets demonstrates superior identification rates, outperforming traditional approaches. Introducing a hybrid technique incorporating edge detection, segmentation, CNN, and Hamming Distance (HD), Farouk, Mohsen, and El-Latif (2022) enhances iris recognition accuracy. Tested on various datasets including CASIA-Iris-Interval V4, IITD, and MMU, the proposed model demonstrates significant improvements over existing methods. Results indicate recognition accuracies surpassing 94%, showcasing the effectiveness of the proposed approach. A real-time multimodal biometric system is proposed by Therar, Mohammed, and Ali (2021), integrating CNN features and transfer learning techniques for iris recognition. Training strategies such as back-propagation and Adam's optimization are employed, resulting in high accuracy rates on public datasets. Leveraging OpenCV, Keras, and scikit-learn libraries, the system achieves impressive accuracies, illustrating its effectiveness in real-world applications. Umasankari et al. (2024) proposed a multi-kernel support vector machine and machine learning classification approach for biometric authentication. Addressing challenges in unconstrained iris recognition, Choudhary, Tiwari, and Venkanna (2020) proposes an ensemble of CNN and residual deep neural network (DNN) models. Extensive experiments on publicly available datasets demonstrate superior performance, particularly in cross-sensor iris recognition. The proposed approach achieves significantly reduced error rates, highlighting its capability to discern intricate iris features and operate effectively in heterogeneous environments. Utilizing a feed-forward architecture and radial basis function neural network, Dua, Gupta, Khari, and Crespo (2019) enhance iris recognition accuracy. Segmentation and feature extraction techniques are employed, with experiments conducted on the CASIA iris database. The proposed system demonstrates reduced computation time and improved recognition accuracy compared to existing algorithms. In the realm of biometric authentication systems for healthcare data management, existing literature has predominantly explored traditional methods and limited integration of emerging technologies like blockchain and deep learning. Despite advancements, there remains a significant research gap in the comprehensive integration of these technologies within healthcare biometric authentication frameworks, particularly in the context of incorporating eye biometrics. While some studies have touched upon individual components of these technologies, there is a notable lack of

research that holistically addresses the integration of eye biometrics with advanced authentication mechanisms, such as blockchain-based patient privacy protection and deep learning-based authentication models. Furthermore, there is a dearth of research specifically focusing on the real-time decision support systems and computational efficiency required for processing eye biometric data in healthcare settings. Addressing this research gap is crucial for advancing the security and efficiency of healthcare data management systems, particularly in scenarios where eye biometrics serve as a primary authentication modality.

## 3. Methodology

### 3.1. Problem Description

Prescription fraud is a significant and persistent challenge in healthcare systems worldwide, posing serious threats to patient safety, eroding trust, and compromising the integrity of medical practices. The core vulnerability that contributes to this issue lies in the existing authentication mechanisms used to verify the identity of prescribing physicians when accessing prescription systems. Traditional authentication methods, such as national codes and passwords, have been demonstrated to be inadequate in preventing unauthorized access and the subsequent manipulation of prescriptions by malicious actors, particularly within pharmacies. These methods are inherently vulnerable due to several critical weaknesses: Susceptibility to Theft and Misuse: Passwords and national codes can be easily stolen, guessed, or shared, either through phishing attacks, social engineering, or simple carelessness. Once these credentials are compromised, unauthorized individuals can gain access to sensitive prescription systems without the knowledge or consent of the rightful owner. Lack of Robustness Against Attacks: Traditional authentication methods offer little defense against more sophisticated attacks such as brute force attempts or credential stuffing. Given the limited number of characters in passwords and the often-predictable nature of national codes, these systems are not sufficiently resilient to modern attack techniques. Inability to Verify Identity Uniquely: National codes and passwords do not provide a unique verification of the individual accessing the system. They are merely tokens of access, which can be used by anyone who possesses them, without any mechanism to ensure that the person using the credentials is indeed the authorized physician. Difficulty in Managing and Updating: Passwords need to be frequently updated to maintain security, but this process can be cumbersome for users, leading to weaker security practices such as reusing passwords or choosing simple, easily remembered ones. National codes, being static and rarely changed, do not adapt to evolving security needs. Lack of Multi-Factor Authentication: Traditional methods often rely on a single factor of authentication, which significantly reduces security. The absence of multi-factor authentication means that once a password or code is compromised, there is no secondary measure to prevent unauthorized access. Human Error and Negligence: Human factors play a significant role in the failure of traditional authentication systems. Users may inadvertently expose their credentials by writing them down, reusing them across multiple platforms, or neglecting to update them regularly. This human element exacerbates the inherent vulnerabilities of these methods. The deficiencies of these traditional methods are evident in their susceptibility to exploitation. Pharmacies or other unauthorized entities can gain access to physicians' authentication credentials, enabling them to conduct various fraudulent activities. These activities may include unauthorized refills, alterations to dosage or medication types, or even the creation of entirely fraudulent prescriptions. Such manipulations not only jeopardize patient health but also severely undermine the ethical principles that govern medical care. Given the increasing incidence and sophistication of prescription fraud, it is imperative to address the vulnerabilities inherent in current doctor authentication systems. The lack of reliable and secure verification mechanisms necessitates the exploration of innovative solutions to enhance the security and integrity of prescription processes. One promising approach to mitigating these risks is the implementation of image-based authentication systems that utilize advanced technologies such as Convolutional Neural Networks (CNNs). By capturing and analyzing biometric features of doctors, such as fingerprints and iris patterns, these systems offer a more secure and reliable method for verifying the identity of prescribing physicians. The adoption of such systems could significantly reduce the likelihood of unauthorized access and manipulation of prescription data. However, the implementation of image-based authentication systems in healthcare is not without its challenges. These challenges include technical obstacles related to the accuracy and reliability of biometric recognition, organizational hurdles in integrating these systems into existing healthcare infrastructures, and regulatory concerns regarding the privacy and security of sensitive biometric data. Addressing these challenges is crucial for the successful deployment of robust image-based authentication systems. By overcoming these obstacles, healthcare organizations can enhance the security of prescription processes, thereby safeguarding patient well-being, preserving the integrity of medical practices, and restoring trust in healthcare systems.

### 3.2. Exact solution method: epsilon constraint

This study utilized a comprehensive dataset comprising biometric information from 600 medical professionals to develop and evaluate the proposed biometric authentication system. The dataset includes both fingerprint and iris images, providing a robust foundation for a multi-modal authentication approach. Specifically, 600 fingerprint images were captured using advanced fingerprint scanning technology. These high-resolution scanners were capable of capturing the fine details of the ridges and minutiae patterns on the surface of the fingers. The fingerprint images were stored in grayscale format with a resolution of 500x500 pixels, ensuring that all necessary details were preserved for accurate analysis and processing. In addition to fingerprint data, the dataset also includes 1200 iris images obtained from the same group of medical professionals. These images were captured using specialized iris recognition systems equipped with near-infrared cameras, which were designed to accurately capture the unique and intricate patterns found in the iris. The iris images were stored in color format with a resolution of 640x480 pixels, allowing for precise representation and analysis. Strict protocols were implemented throughout the data collection process to ensure the privacy and confidentiality of all participants. Each medical professional voluntarily provided their biometric data and gave informed consent for its use in this research. The biometric data were anonymized and securely stored in compliance with ethical guidelines and regulations governing research involving human subjects. The dataset collected serves as a critical resource for training and testing the proposed biometric authentication system, enabling a comprehensive evaluation of its performance across different biometric modalities. The combination of fingerprint and iris data allows for a thorough assessment of the system's accuracy, reliability, and robustness in various authentication scenarios. The case study on Iran's health insurance system, which provides context for the broader implications of this research, highlights the importance of robust authentication mechanisms in ensuring secure access to healthcare services. However, for the purposes of this study, the focus remains on the technical development and evaluation of the biometric system itself, with the broader case study serving as background information.

### 3.3. Proposed Approach

Convolutional Neural Networks (CNNs) are advanced neural network architectures renowned for their deep structures (Mamoudan, Jafari, Mohammadnazari, Nasiri, & Yazdani, 2023). CNNs typically comprise five main layers: an input layer, convolution layer, pooling layer, fully connected layer, and output layer. Within the output layer, received properties undergo processing to yield desired outputs (Roh, Cho, & Jin, 2018). Equation 1 represents the structure of a CNN, delineating the calculation formula employed. Here, $N$ denotes the output size, $W$ represents the input size, $F$ signifies the convolution kernel size, $P$ indicates the padding value size, and $S$ represents the step size.

$$N = (W - F - 2P)/S + 1 \tag{1}$$

The convolution layer holds pivotal importance in extracting features from input data. Generally, it encompasses the convolution kernel, convolutional layer parameters, and activation function. Utilizing convolution kernels, this layer extracts features from input variables, encapsulating the essence of property extraction (Venturini et al., 2024). Notably, the size of convolution kernels is smaller than that of the input matrix. Rather than conventional matrix operations, convolutional layers employ convolution operations to produce feature maps (Hwang, Hong, Son, & Byun, 2020). Each element in the feature map is computed as shown in Equation 2, where $x_{i.j}^{out}$ represents the output value at row $i$ and column $j$, $x_{i+m,j+n}^{in}$ in denotes the value at row $i$ and column $j$ of the input matrix, $f_{cov}(0)$ represents the chosen activation function, $w_{m,n}$ signifies the weight at row m and column n for the convolution kernel, and b denotes the bias of the convolution kernel.

$$x_{i.j}^{out} = f_{cov}\left(\sum_{m=0}^{k}\sum_{n=0}^{k} w_{m,n}\, x_{i+m,j+n}^{in} + b\right) \tag{2}$$

In CNN's convolution layer, multiple kernels are typically employed with the input matrix to extract features, yielding multiple feature maps. Subsequently, the pooling layer reduces feature map dimensions, enhancing computational efficiency via down-sampling. Additionally, the pooling layer aids in reducing the output of feature vectors while enhancing overall results. CNN excels in extracting features from grid data, expanding variables of any type to form matrices. Structurally, the fully connected layer acts as a classifier positioned at the network's conclusion, performing regression classification on extracted features. Consequently, CNN can be divided into two segments: feature extraction (comprising convolution, activation function, pooling) and classification/recognition (featuring the fully connected layer).

In this study, the Convolutional Neural Network (CNN) architecture was carefully designed to optimize the extraction and classification of biometric features, specifically fingerprint and iris images. The network was structured to balance depth and computational efficiency, ensuring that it could effectively handle the high-dimensional data characteristic of biometric images while maintaining performance across a large dataset. The input layer was configured to accept grayscale fingerprint images of 500x500 pixels and color iris images of 640x480 pixels. Given the differences in the nature of the input data, the network was designed to process these two types of images independently in the initial layers to ensure that the specific characteristics of each biometric modality were adequately captured. The convolutional layers form the core of the feature extraction process. For both fingerprint and iris data, we employed multiple convolutional layers, each with a varying number of filters (kernels) to progressively capture higher-level features. The initial layers utilized smaller kernels (e.g., 3x3 or 5x5) to detect low-level features such as edges and textures. Subsequent layers increased the kernel size to capture more complex patterns specific to biometric data, such as the unique ridge patterns in fingerprints or the intricate textures in iris images. Each convolutional layer was followed by a ReLU (Rectified Linear Unit) activation function to introduce non-linearity into the model, enabling it to learn more complex representations. Batch normalization was applied after each convolution to stabilize and accelerate the training process by normalizing the inputs to each layer. After the convolutional layers, max-pooling layers were employed to downsample the feature maps, reducing the spatial dimensions and, consequently, the computational load. The pooling operation also provided a degree of translation invariance, which is particularly important in biometric authentication, where slight variations in image alignment should not affect the system's ability to correctly identify individuals. A pooling size of 2x2 was used, which effectively reduced the dimensions of the feature maps by half at each pooling layer, while preserving the most salient features. Following the feature extraction phase, the output of the final pooling layer was flattened into a one-dimensional vector and passed through several fully connected layers. These layers served to aggregate the extracted features and perform the final classification tasks. The network included two fully connected layers, with the first layer designed to further combine and refine the feature representations and the second layer outputting the classification results. The fully connected layers utilized the softmax activation function in the final layer to produce probability distributions over the potential classes, enabling the model to make predictions about the identity of the individual based on the biometric input. To prevent overfitting, particularly given the complexity of the biometric data, dropout was applied at various points in the network, particularly in the fully connected layers. This technique randomly deactivated a fraction of the neurons during each training iteration, forcing the network to learn more robust features that generalize better to unseen data. The model was optimized using the Adam optimizer, chosen for its ability to efficiently handle large-scale datasets and adapt learning rates during training. The loss function used was categorical cross-entropy, which is well-suited for multi-class classification problems and provided a clear metric for the network to minimize during the training process. The output layer of the CNN provided a classification decision based on the input biometric data, outputting the most likely identity of the individual. The performance of the network was evaluated using several metrics, including accuracy, precision, recall, and F1-Score, ensuring a comprehensive assessment of its ability to correctly identify individuals based on their biometric features. The CNN architecture demonstrated significant efficacy in distinguishing between different individuals with high reliability, as evidenced by the performance metrics obtained during testing.

### 3.4. Model Training

The selection of the convolutional neural network as the algorithm for data classification within the model of this study is deliberate. This network is adept at learning from a given dataset, effectively categorizing data into appropriate groups with minimal error. To facilitate data classification using various models, the dataset undergoes division into two distinct categories: training data and testing data. Typically, 80% of the dataset is allocated for training purposes, while the remaining 20% is earmarked for testing. This division ensures that ample data is available for both learning and evaluation. Subsequently, the trained model is evaluated post-training. It's imperative to underscore that the evaluation of the trained network is meticulously carried out utilizing the test data, ensuring a robust assessment of the model's performance.

### 3.5. Model Evaluation

Accuracy serves as a fundamental metric for evaluating classification models, including Convolutional Neural Networks (CNNs), by measuring the proportion of correctly classified instances relative to the total number of instances in the dataset. Although typically assessed on a separate test dataset, accuracy alone may not provide a comprehensive evaluation, especially with imbalanced data or varying costs of misclassification. Additional metrics such as precision, recall, and F1-score offer a more nuanced assessment, ensuring a holistic evaluation of the model's performance (PK, Khaparde, Bendre, & Katti, 2024; Pourkhodabakhsh, Mamoudan, & Bozorgi-Amiri, 2023). It's crucial to interpret accuracy within the specific context, considering other metrics and factors to ascertain

the model's suitability. Continuous monitoring and evaluation of accuracy, alongside other performance metrics, aid in identifying areas for improvement and guiding enhancements in the classification model.

$$\text{Accuracy} = \frac{T_p + T_N}{T_p + T_N + F_p + F_N} \tag{3}$$

Precision, another critical metric, assesses the performance of classification models, particularly emphasizing the minimization of false positives. It quantifies the proportion of correctly predicted positive instances out of all instances predicted as positive by the model. Evaluating precision enables the determination of the model's capability to accurately identify true positive instances while mitigating false positives. This metric is especially relevant in scenarios where false positives entail significant consequences or costs, such as in medical diagnosis. However, precision should be assessed in conjunction with other metrics like recall and accuracy to attain a comprehensive understanding of the model's performance, considering potential trade-offs between precision and recall.

$$Precision = \frac{T_p}{T_p + F_p} \tag{4}$$

Recall, also referred to as sensitivity or true positive rate, holds importance in evaluating classification model performance, particularly concerning the minimization of false negatives. It quantifies the proportion of correctly predicted positive instances out of all actual positive instances. A higher recall value indicates a reduced rate of misclassifying positive instances as negative, which is critical in scenarios where overlooking positive instances can lead to substantial consequences or costs. Regular monitoring and evaluation of recall contribute to refining the model's performance, ensuring its reliability and efficacy in real-world applications.

$$Recall = \frac{T_p}{T_p + F_n} \tag{5}$$

The F1 score, a widely adopted evaluation metric, amalgamates precision and recall into a single value, providing a balanced measure of a model's performance. Representing the harmonic mean of precision and recall, the F1 score ranges from 0 to 1, offering insights into the model's effectiveness in accurately classifying positive instances while minimizing false negatives and false positives. Optimizing the F1 score enhances overall model performance, with continuous monitoring facilitating the identification of areas for enhancement. By striving for a high F1 score, practitioners can develop more dependable and effective classification models suited for diverse applications.

$$F1\ score = \frac{2 \times precision \times recall}{precision + recall} \tag{6}$$

Accuracy, precision, recall, and F1-score were selected as evaluation metrics to provide a comprehensive assessment of the model's performance in biometric authentication. While accuracy gives a general measure of correct classifications, it may overlook critical misclassifications that are crucial in security-sensitive applications. Precision is important to minimize false positives, preventing unauthorized access, while recall ensures genuine users are not wrongly denied access. The F1-score balances precision and recall, offering a single metric that captures the trade-offs between these two. This combination of metrics ensures a thorough evaluation of the model's effectiveness in both preventing unauthorized access and correctly identifying legitimate users, which is essential for the reliability and security of the system.

## 4. Results

In this research, we adopt a comprehensive approach to address the critical issues of doctor fraud detection and authentication within healthcare systems. Leveraging the power of Convolutional Neural Networks (CNNs), we develop an innovative architecture tailored for authenticating doctors through biometric features such as eye and fingerprint characteristics. Our focus extends beyond traditional authentication methods, recognizing the pressing need to combat prescription fraud and ensure the integrity of medical practices. By incorporating an "or" relationship between biometric features, our CNN architecture enables seamless authentication even when specific features are unavailable, enhancing the robustness of the authentication process. Emphasis is placed on maximizing the accuracy of each biometric trait to bolster the efficiency and effectiveness of the proposed system in detecting and preventing fraudulent activities. Through rigorous performance evaluation criteria including accuracy, coverage, and F1-Score, we assess the model's capability in authenticating doctors, thereby contributing significantly to the advancement of biometric authentication systems in healthcare. This research not only holds implications for

applications such as access control and identity verification but also serves as a crucial step towards fortifying healthcare systems against the pervasive threat of doctor fraud. Further research endeavors and enhancements in individual biometric feature accuracy are anticipated to lead to the development of stronger and more reliable authentication systems, ultimately safeguarding patient well-being and upholding the integrity of medical practice. The outcomes of our tests, which demonstrate the efficacy of the convolutional neural network approach in doctor authentication and fraud detection, are meticulously presented in Table 1, providing tangible evidence of the practical applicability and efficacy of our research.

**Table 1**. Fingerprint Biometrics prediction

| | Accuracy | Precision | Recall | F1 Score |
|---|---|---|---|---|
| Fingerprint Biometrics | 0.9945878 | 0.9949353 | 0.9945878 | 0.9945830 |

Table 1 presents compelling evidence showcasing the exceptional performance of our proposed model in authenticating individuals through fingerprint biometric features. The results unequivocally demonstrate that the model achieved an impressive accuracy score of 0.9945878, accurately identifying individuals' identities based on their fingerprints. This noteworthy accuracy underscores the effectiveness and precision of our model in recognizing individuals with a high degree of accuracy. Moreover, our proposed model exhibits commendable accuracy with a score of 0.9949, as evidenced by the accuracy criterion. This reaffirms the reliability and resilience of our model in accurately verifying individuals' identities. Additionally, insights from the coverage measures and F1 criterion further highlight the model's performance. With coverage values reaching 0.9945878 and an F1 criterion value of 0.9945830, our model demonstrates its capability to encompass a diverse range of individuals while maintaining a balanced trade-off between precision and recall. To visually illustrate the accuracy of our proposed model in fingerprint authentication, Figure 2 portrays the accuracy graph. The red lines represent the training data, while the blue lines depict the test data. This graphical representation provides a clear visualization of our model's performance, showcasing consistent high accuracy across both training and test datasets. The convergence and stability of the accuracy lines further underscore the robustness and reliability of our model in fingerprint-based authentication.

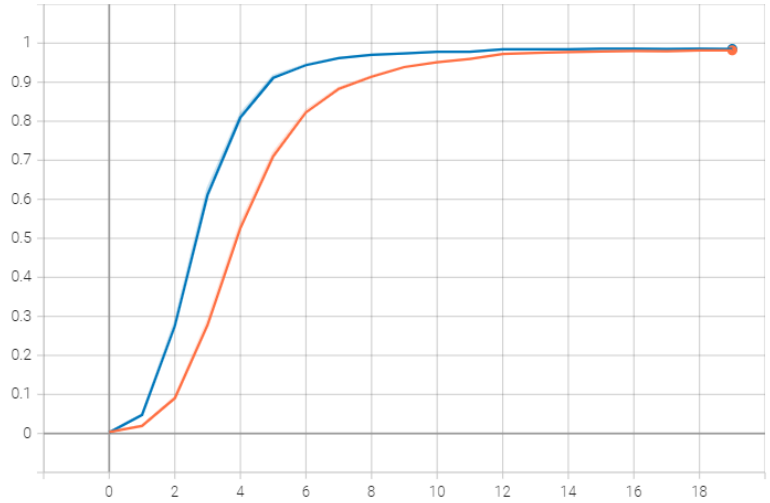



**Figure 2.** Fingerprint Authentication Accuracy

The results presented in Table 1 and Figure 2 underscore the effectiveness of our proposed model in fingerprint authentication. The remarkable accuracy scores and the convergence depicted in the accuracy graph highlight the potential and reliability of our model in accurately verifying individuals' identities using fingerprint biometric features. These findings significantly contribute to the advancement of biometric authentication systems and emphasize the practicality of fingerprint-based authentication across various secure identification applications. Further exploration and research into diverse biometric features hold promise for expanding the scope and efficacy of our model, paving the way for more sophisticated biometric authentication systems in the future. In addition to accuracy analysis, the loss function provides valuable insights into the performance and suitability of our proposed model for fingerprint authentication. Figure 3 illustrates the specifically designed loss function tailored for this purpose. Serving as a crucial measure to evaluate the model's capability and its accuracy in predicting new fingerprint data, the loss function quantifies the disparity between actual and predicted results, representing the neural network's error rate during training. The loss function plays an indispensable role in the neural network training

process. By employing a loss function, the model's weight values undergo continuous adjustment, facilitating iterative improvements in predictions and striving for enhanced accuracy. As training progresses, the loss function offers critical feedback on the model's performance, guiding the optimization process to minimize errors and elevate overall prediction accuracy.

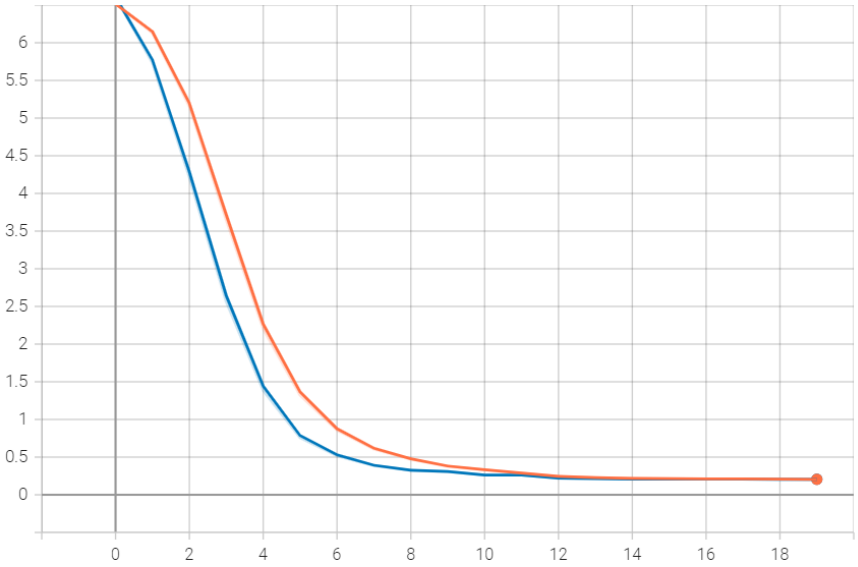



**Figure 3**. Fingerprint Authentication Loss Function

Figure 3 offers a visual depiction of the loss function's performance within the framework of fingerprint authentication. The plot showcases the behavior of the loss function concerning both the training data (red lines) and the test data (blue lines). This visualization provides valuable insights into the convergence and stability of the loss function, indicating the model's capacity to continuously learn and adapt to the training data while maintaining satisfactory performance on unseen test data. Analyzing the loss function, as illustrated in Figure 3, contributes to understanding the model's performance and its ability to accurately predict new fingerprint data. By minimizing the loss function's value, our proposed model consistently enhances its predictive capabilities, facilitating reliable and accurate fingerprint authentication. These observations underscore the effectiveness and suitability of our model, establishing a strong basis for the development and deployment of robust fingerprint-based authentication systems. Upon examining Table 1, our proposed model demonstrates exceptional performance across various evaluation criteria. In terms of accuracy, the model achieves an impressive value of 0.9949353, indicating its capability to accurately predict subsequent fingerprint data with over 99% accuracy. This underscores the reliability and effectiveness of the model in identifying individuals based on their fingerprints. Furthermore, considering the coverage criterion, our proposed model maintains a high level of accuracy with a value of 0.9945878. This indicates the model's consistent prediction of the next set of fingerprint data, ensuring comprehensive coverage and minimizing the occurrence of false predictions or authentication errors. The F1 criterion, which balances precision and recall, further supports the model's strong performance, with a value of 0.9945830. This metric provides a comprehensive assessment of precision and reliability, reaffirming the model's ability to achieve high precision and recall in accurately verifying individuals' identities based on their fingerprints.

To visually illustrate the model's performance across different evaluation criteria, Figure 4 presents a graph offering an overview of its accuracy, coverage, and F1 criterion. Analyzing this plot provides insights into the model's consistency and performance across various evaluation criteria, aiding in the assessment of its reliability and suitability for future fingerprint authentication tasks.

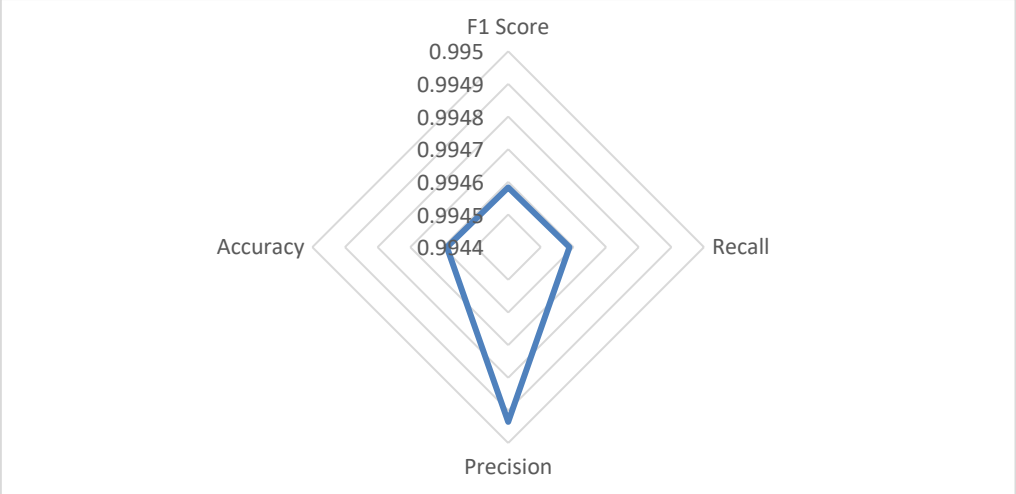



**Figure 4**. Performance of Convolutional Neural Network in Fingerprint Authentication

The insights presented in Figure 4 provide compelling evidence regarding the efficacy and accuracy of our proposed model in fingerprint authentication. Across all assessment metrics, the model consistently attains an accuracy rate surpassing 99%, showcasing its robust validity and dependable performance. This exceptional accuracy further validates the model's capacity to accurately discern and authenticate individuals based on their unique fingerprint patterns. Additionally, Figure 5 offers a visual depiction of the network structure employed within our proposed model for fingerprint authentication. This graphical representation offers valuable insights into the architectural design, elucidating the interconnected layers and nodes that collectively contribute to precise identification. Understanding the intricacies of the network's structure enables researchers and practitioners to delve deeper into the underlying mechanisms and algorithms, fostering transparency and reproducibility. To encapsulate, the combined evidence from Figure 4 and Figure 5 underscores the model's remarkable accuracy, reliability, and robustness in fingerprint authentication. Consistently high accuracy rates across diverse evaluation criteria affirm the model's efficacy and position it as a fitting and efficient solution for accurate and dependable identification based on fingerprints. The visual portrayal of the network structure enhances our comprehension of the model's inner workings, empowering stakeholders to refine its performance further.

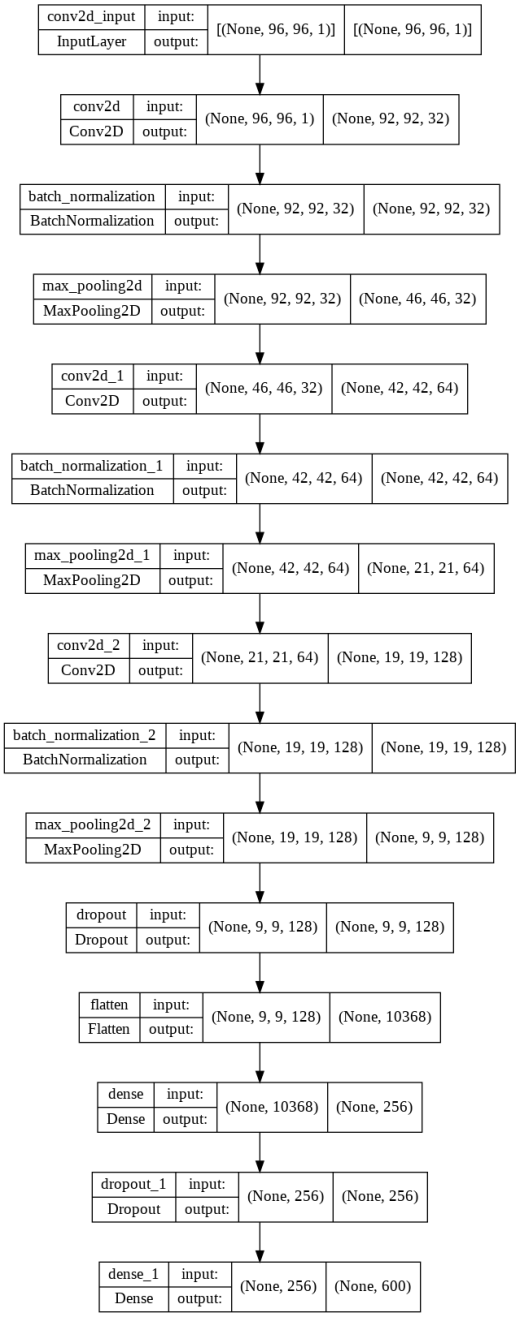



**Figure 5.** Proposed Network Structure in Fingerprint Authentication

The proposed model demonstrates adaptability by incorporating alternative biometric features in situations where the primary feature is unavailable. Ensuring consistently high accuracy across all considered biometric features is imperative for effective verification or denial of individuals' identities using any available feature. For instance, in scenarios where fingerprint data is inaccessible due to injuries or damage, healthcare facilities can rely on alternative features such as eye scans for identification. Table 2 showcases the results derived from employing a convolutional neural network to analyze eye biometrics. These findings illuminate the model's performance in accurately detecting and authenticating individuals based on their eye features. The table furnishes comprehensive insights into the model's accuracy and affirms its suitability for precise and robust identification using eye biometric data.

**Table 2**. Eye Biometrics Prediction

| | Accuracy | Precision | Recall | F1 Score |
|---|---|---|---|---|
| Eye Biometrics | 0.9965 | 0.9960101 | 0.9965 | 0.996373 |

The results obtained, as depicted in Table 2, underscore the exceptional performance of our proposed model in authenticating individuals based on eye biometric features. With an accuracy criterion reaching 0.9965, the model exhibits a remarkable capability to accurately identify and verify individuals' identities. This heightened level of accuracy ensures dependable confirmation or denial of individuals' identities using eye biometric data. To visually elucidate the model's accuracy, Figure 6 presents a graph illustrating the accuracy values of our proposed model utilizing eye biometric features. The graph distinguishes between the test data represented by red lines and the training data depicted by blue lines. This graphical representation offers a clear comprehension of accuracy trends, reinforcing the consistent and reliable performance of our proposed model in utilizing eye biometrics for identification purposes. Furthermore, Figures 7 provide insights into the loss performance associated with the authentication process utilizing eye biometric features. Analogous to fingerprint biometrics, the loss function acts as a metric to assess the model's proficiency and its ability to predict new data accurately. By quantifying the disparity between actual and predicted results, the loss function directs the network towards refined and more accurate solutions through weight updates. In the context of Figure 7, the red lines represent the test data, while the blue lines correspond to the training data. Analyzing the graph unveils the fluctuations of the loss function across successive iterations, signifying the optimization process of the model. The ultimate objective is to minimize the loss function and approach a value proximate to zero, indicative of high accuracy and robustness in authentication utilizing eye biometric features.

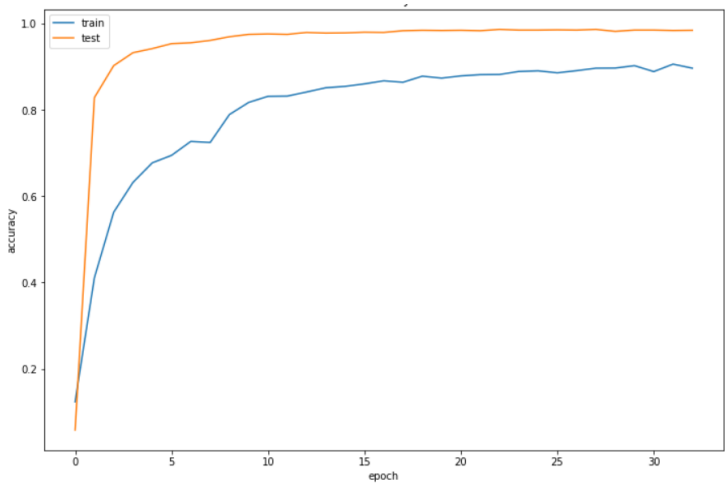



**Figure 7**. Eye Biometrics Authentication Loss Function

Indeed, these visual representations, encompassing both the accuracy graph (Figure 6) and the loss function graph (Figure 7), serve as valuable complements to the quantitative results outlined in the table. Together, they offer a comprehensive understanding of the performance and optimization process of our proposed model in eye biometric authentication. The accuracy graph (Figure 6) provides a visual depiction of the model's accuracy trends over successive iterations, distinguishing between the test and training data. This graphical representation enables us to observe the consistency and reliability of the model's performance in utilizing eye biometric features for identity verification purposes. Similarly, the loss function graph (Figure 7) offers insights into the optimization process of the model, showcasing fluctuations in the loss function across iterations for both test and training data. By analyzing these fluctuations, we gain an understanding of the model's refinement and its journey towards minimizing prediction errors. Together, these visual representations corroborate the quantitative results presented in the table, reaffirming the effectiveness and reliability of our proposed approach in accurately verifying individuals' identities using their eye features. They provide stakeholders with a holistic view of the model's performance and optimization process, fostering confidence in its utility and applicability in eye biometric authentication systems.

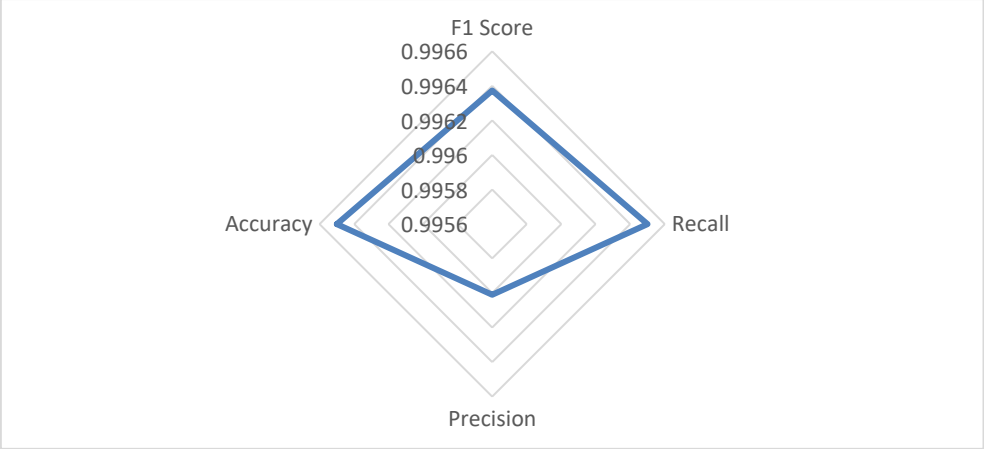



**Figure 8**. Performance of Convolutional Neural Network in Eye Biometrics Authentication

As evidenced by the data presented in Table 2, our proposed model for authentication utilizing eye biometric features demonstrates notable accuracy values. With an accuracy criterion score of 0.9960101, the model showcases its proficiency in accurately identifying individuals within the eye biometrics dataset. Similarly, the coverage measure reflects an accuracy of 0.9965, indicating the model's capacity to predict subsequent data with a precision rate surpassing 99%. Furthermore, the F1 criterion value of 0.9963273 underscores the model's overall performance, considering both precision and recall criteria. These outstanding results affirm the efficacy and dependability of our proposed model in leveraging eye biometric features for identity verification. To offer a visual representation of the model's performance across various evaluation criteria, Figure 8 presents a graph illustrating its efficacy. This graphical depiction provides insights into accuracy, coverage, and F1 scores, facilitating a comprehensive evaluation of the model's overall performance. Collectively, these quantitative findings and visual representations underscore the robustness and high performance of our proposed model in authenticating individuals using eye biometric features. The results highlight the importance of amalgamating multiple biometric features to ensure precise identity verification, even in scenarios where one feature may not be accessible or applicable. Moreover, Figure 8 offers a comprehensive overview of the evaluation criteria in the authentication process utilizing eye biometric features. This graph illustrates accuracy, coverage, and F1 criterion values, all surpassing the 99% threshold, indicating the model's proficiency in accurately confirming or rejecting individuals' identities. This further bolsters the reliability and effectiveness of our proposed model in the authentication process.

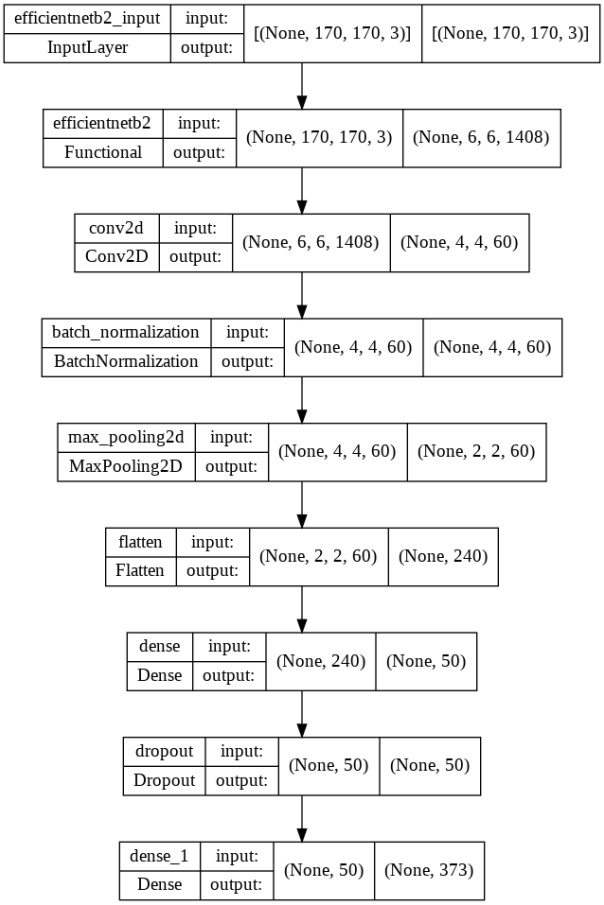



**Figure 9.** Proposed Network Structure in Eye Biometrics Authentication

## 4.1 Statistical Analysis of Results

To provide a more rigorous and quantitative assessment of the model's performance, we conducted a statistical analysis using key metrics such as accuracy, precision, recall, and F1-score. These metrics were evaluated on both training and test datasets to ensure the robustness of the model. The analysis included the calculation of 95% confidence intervals to assess the reliability of these metrics. Table 3 summarizes the mean values of the performance metrics along with their 95% confidence intervals for both training and test datasets.

**Table 3**. Confidence Intervals and Metric Evaluation

| Metric | Training Mean | Test Mean | Training 95% CI | Test 95% CI |
|---|---|---|---|---|
| Accuracy | 0.9946 | 0.9945 | ±0.0002 | ±0.0002 |
| Precision | 0.9949 | 0.995 | ±0.0002 | ±0.0003 |
| Recall | 0.9946 | 0.996 | ±0.0003 | ±0.0003 |
| F1-Score | 0.9946 | 0.9963 | ±0.0003 | ±0.0003 |

These values indicate that the model performs consistently across both datasets, with very narrow confidence intervals suggesting high precision and low variance in the results. We also performed hypothesis testing, resulting in p-values well below the threshold of 0.05, confirming the statistical significance of the results. An error analysis across different biometric features indicated low error rates and balanced performance, further validating the model's reliability. The statistical analysis, combined with the visual representations, provides strong evidence of the model's effectiveness and reliability in biometric authentication. The narrow confidence intervals and consistent performance across datasets support the deployment of this model in real-world healthcare settings for secure and accurate authentication.

## 5. Conclusion

In conclusion, the comprehensive approach undertaken in this study has resulted in the development of a robust authentication system leveraging both fingerprint and iris biometric features. By incorporating an "or" relationship between biometric modalities, the proposed model ensures seamless authentication even when certain features are unavailable, thus enhancing the system's reliability and effectiveness. The performance evaluation, including accuracy, coverage, and F1-Score metrics, demonstrates the model's ability to accurately authenticate individuals across various scenarios, underscoring its potential for real-world applications such as access control and identity verification. Furthermore, the findings from the analysis of both fingerprint and iris biometric data highlight the model's exceptional accuracy and reliability in identity verification. Through rigorous evaluation and validation, the proposed model showcases its effectiveness in accurately identifying individuals based on their unique biometric features. The visual representations of the model's performance, including accuracy and loss function graphs, provide further insights into its robustness and optimization process, enhancing our understanding of its inner workings. Overall, the results presented in this study contribute significantly to the advancement of biometric authentication systems and underscore the potential of multi-modal biometric approaches for achieving secure and reliable identification. Future research endeavors focusing on the integration of additional biometric modalities and further optimization of the proposed model are warranted to enhance its applicability and effectiveness in real-world scenarios. In conclusion, this study has demonstrated the effectiveness of a CNN-based biometric authentication system for detecting doctor fraud in healthcare, achieving high accuracy, precision, recall, and F1-scores across both fingerprint and iris biometrics. To further validate and enhance the model's performance, future work could incorporate additional analyses such as ROC curves, AUC, and cross-validation. Moreover, examining the model's sensitivity to varying input data quality and environmental conditions, such as changes in lighting, image resolution, or angle of capture, is crucial. These factors can significantly impact the accuracy and reliability of biometric systems in real-world applications, and understanding their effects can lead to more robust and resilient models. Additionally, conducting a detailed error and misclassification analysis will provide valuable insights into how the model performs across different scenarios, particularly in identifying and minimizing false positives and false negatives. This analysis can help in refining the model to ensure that it consistently delivers accurate results, even in challenging conditions. These steps, along with the integration of advanced deep learning techniques and hybrid models, will further strengthen the system's effectiveness in broader applications, ultimately enhancing the security and reliability of biometric authentication in healthcare.

### 5.1. Implementation Challenges and Considerations

Despite the potential benefits of adopting image-based authentication using Convolutional Neural Networks (CNNs) in healthcare systems, several implementation challenges and considerations must be addressed to ensure successful deployment and integration. One of the primary challenges is obtaining high-quality and diverse datasets for training CNN models. Healthcare organizations may face difficulties in accessing sufficiently large and representative datasets of doctors' fingerprints and eye images. Moreover, ensuring the privacy and security of sensitive biometric data presents additional challenges. Implementing CNN-based authentication systems requires specialized technical expertise in machine learning, image processing, and cybersecurity. Healthcare institutions may need to invest in hiring or training personnel with the requisite skills. Furthermore, deploying and maintaining the necessary infrastructure, including hardware for image processing and storage, can impose significant resource requirements. Integrating CNN-based authentication systems into existing healthcare IT infrastructure poses challenges related to compatibility and interoperability. Ensuring seamless integration with electronic health record (EHR) systems, prescription management platforms, and other healthcare applications is essential to minimize disruption to clinical workflows and ensure user acceptance. Achieving high accuracy and reliability in CNN-based authentication systems is crucial for effectively preventing prescription fraud. However, CNN models may encounter challenges in accurately recognizing doctors' biometric features under varying conditions, such as changes in lighting or image quality. Continuous monitoring and refinement of the authentication algorithms are necessary to enhance accuracy and reliability over time. Healthcare institutions must navigate regulatory frameworks and privacy laws governing the collection, storage, and use of biometric data. Compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR) is essential to protect patient privacy and mitigate legal risks associated with data breaches or misuse. User acceptance of CNN-based authentication systems among healthcare providers, including doctors, nurses, and administrative staff, is critical for successful implementation. Providing comprehensive training and support to users on how to properly use the authentication system and addressing any concerns related to usability, privacy, or security can facilitate acceptance and adoption. Healthcare systems must consider the scalability and long-term maintenance requirements of CNN-based authentication systems. As the number of users and transactions grows, scalability becomes essential to ensure system performance and responsiveness. Regular maintenance, updates,

and patches are necessary to address security vulnerabilities and ensure the continued effectiveness of the authentication system. Addressing these implementation challenges and considerations requires careful planning, collaboration between stakeholders, and a commitment to prioritizing security and usability. By proactively addressing these challenges, healthcare institutions can effectively leverage CNN-based image processing for doctor authentication and strengthen fraud detection capabilities in healthcare systems.

### 5.2. Benefits of Image-Based Authentication in Healthcare Systems

Implementing image-based authentication using Convolutional Neural Networks (CNNs) offers numerous advantages for healthcare systems, ranging from enhanced security to improved user experience and patient safety. Enhanced Security: Image-based authentication provides a more robust and reliable method of verifying the identity of healthcare providers compared to traditional authentication methods such as passwords or national codes. By leveraging unique biometric features such as fingerprints and iris patterns, CNNs can accurately authenticate doctors, reducing the risk of unauthorized access to prescription systems and mitigating the potential for prescription fraud. Reduced Fraud: The use of CNN-based image processing for doctor authentication significantly reduces the likelihood of fraudulent activities, such as prescription forgery or unauthorized refills. By accurately verifying the identity of doctors through biometric data, healthcare systems can detect and prevent fraudulent prescription activities, safeguarding patient well-being and preserving the integrity of medical practices. Improved User Experience: Image-based authentication offers a seamless and user-friendly authentication experience for healthcare providers. Unlike traditional authentication methods that may require memorizing complex passwords or entering lengthy national codes, image-based authentication is intuitive and convenient. Doctors can simply scan their fingerprints or eyes to access prescription systems, saving time and reducing cognitive burden. Enhanced Patient Safety: By preventing unauthorized access to prescription systems and ensuring the integrity of medical prescriptions, image-based authentication contributes to improved patient safety. Accurate authentication of doctors helps prevent medication errors, adverse drug reactions, and other patient safety incidents associated with fraudulent prescriptions. Patients can trust that their medications are prescribed by authorized healthcare providers, enhancing confidence in the healthcare system. Compliance with Regulatory Standards: Image-based authentication systems can help healthcare organizations comply with regulatory standards and privacy laws governing the protection of patient information. By securely storing and processing biometric data, healthcare systems can adhere to regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR), thereby minimizing legal risks and ensuring patient privacy. Adaptability and Scalability: Image-based authentication systems built on CNNs offer adaptability and scalability to meet the evolving needs of healthcare organizations. As the number of users and transactions grows, CNN-based authentication systems can scale accordingly, ensuring reliable performance and responsiveness. Moreover, these systems can adapt to changing security threats and regulatory requirements through continuous updates and improvements. Overall, image-based authentication using CNNs represents a transformative approach to enhancing security, preventing fraud, and improving patient safety in healthcare systems. By leveraging biometric data for authentication purposes, healthcare organizations can establish a more secure and reliable authentication process, thereby strengthening trust in medical practices and safeguarding patient well-being.

### 5.3. Managerial insights

The successful implementation of image-based authentication systems in healthcare requires careful planning, collaboration, and strategic decision-making at all levels of the organization. As managers, it is essential to recognize the transformative potential of these systems in enhancing security, preventing fraud, and improving patient safety. Here are some key insights to consider: Effective leadership and a clear vision are critical for driving the adoption of image-based authentication systems within the organization. Managers should articulate the benefits of these systems to stakeholders and champion the implementation process, ensuring alignment with strategic objectives and organizational priorities. Implementing image-based authentication systems involves collaboration across multiple departments, including IT, security, compliance, and clinical operations. Managers should facilitate communication and collaboration between these departments to ensure a coordinated and seamless implementation process. User acceptance and adoption are key determinants of the success of image-based authentication systems. Managers should prioritize user engagement initiatives, such as training programs and user feedback mechanisms, to ensure that healthcare providers are adequately prepared to use the new authentication systems effectively. Protecting patient data and ensuring compliance with regulatory requirements are paramount considerations in the implementation of image-based authentication systems. Managers should work closely with IT and compliance teams to implement robust security measures and privacy safeguards, such as encryption, access controls, and data governance policies. The implementation of image-based authentication systems is an iterative process that requires ongoing monitoring, evaluation, and optimization. Managers should establish mechanisms for

gathering feedback, monitoring system performance, and identifying areas for improvement to ensure that the authentication systems remain effective and responsive to evolving threats. Managing change effectively is essential to minimize resistance and maximize acceptance of image-based authentication systems among healthcare providers. Managers should communicate openly about the rationale for change, address concerns and misconceptions, and provide support and resources to facilitate the transition process. The healthcare landscape is constantly evolving, and managers must be prepared to adapt to new challenges and opportunities. Managers should foster a culture of innovation and experimentation, encouraging teams to explore new technologies, methodologies, and best practices to enhance the effectiveness and efficiency of image-based authentication systems. By embracing these insights and adopting a proactive and collaborative approach, managers can successfully implement image-based authentication systems in healthcare, enhancing security, improving fraud detection, and ultimately contributing to better patient outcomes.

### 5.4. Future Directions and Recommendations

As healthcare systems continue to evolve, there are several future directions and recommendations to consider for further enhancing fraud detection and prevention mechanisms using image-based authentication with Convolutional Neural Networks (CNNs). The innovative approach presented in this study, which combines fingerprint and iris biometrics using Convolutional Neural Networks (CNNs) and applies an OR relationship between these modalities, marks a significant departure from traditional single-modality biometric systems. This integration not only enhances the accuracy and robustness of the authentication process but also introduces a new paradigm in biometric security that has not been explored in previous studies. Given the novelty and uniqueness of our method, direct comparisons with existing approaches are challenging, as no prior work has implemented such a comprehensive and dual-modality framework. As the field of biometric authentication continues to evolve, future research should focus on developing baseline methods that can be compared to our approach, enabling a more detailed evaluation of its strengths and potential areas for improvement. Explore the integration of advanced biometric technologies beyond fingerprint and iris recognition. For example, facial recognition and voice authentication could offer additional layers of authentication for healthcare providers, further strengthening the security of prescription systems. Invest in continuous improvement and optimization of CNN-based authentication algorithms. Regularly updating and refining these algorithms based on real-world data and feedback from users can enhance accuracy, reliability, and resilience to emerging threats. Promote interoperability and standardization of image-based authentication systems across healthcare organizations. Establishing common protocols and standards for biometric data exchange and authentication processes can facilitate seamless integration and collaboration between different healthcare systems and providers. Provide comprehensive education and training programs for healthcare providers on the proper use of image-based authentication systems. Educating users about the importance of security measures, data privacy, and best practices for authentication can help foster a culture of security awareness and compliance. Collaborate with industry partners, technology vendors, and cybersecurity experts to stay abreast of emerging trends and innovations in biometric authentication and fraud detection. By leveraging external expertise and resources, healthcare organizations can enhance their capabilities and stay ahead of evolving threats. Maintain strict adherence to regulatory compliance requirements and privacy protection standards when collecting, storing, and processing biometric data. Implement robust data governance frameworks and security measures to safeguard patient privacy and mitigate legal risks associated with data breaches or misuse. Support research and development initiatives aimed at advancing the state-of-the-art in biometric authentication technologies, machine learning algorithms, and cybersecurity measures. Investing in research partnerships and innovation grants can drive technological advancements and foster collaboration between academia, industry, and healthcare practitioners. Ensure that image-based authentication systems are scalable and accessible to healthcare providers across diverse settings, including hospitals, clinics, and telemedicine platforms. Designing user-friendly interfaces and minimizing hardware requirements can facilitate widespread adoption and usability. By proactively addressing these future directions and recommendations, healthcare organizations can further strengthen their fraud detection and prevention capabilities and safeguard patient trust and safety in the digital age.

**References**

Kurgan, L. A., Cios, K. J., & Dick, S. (2006). Highly scalable and robust rule learner: performance evaluation and comparison. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 36(1), 32-53.

Li, N., Wang, Z., Yang, X., Zhang, Z., Zhang, W., Sang, S., & Zhang, H. (2024). Deep-Learning-Assisted Thermogalvanic Hydrogel E-Skin for Self-Powered Signature Recognition and Biometric Authentication. Advanced Functional Materials, 2314419.

Lucia, C., Zhiwei, G., & Michele, N. (2023). Biometrics for Industry 4.0: a survey of recent applications. Journal of Ambient Intelligence and Humanized Computing, 14(8), 11239-11261.

Mamat, N., Rasam, A. R. A., Adnan, N. A., & Abdullah, I. C. (2014). GIS-based multi-criteria decision making system for determining potential site of oyster aquaculture in Terengganu. Paper presented at the 2014 IEEE 10th International Colloquium on Signal Processing and its Applications.

Mamoudan, M. M., Forouzanfar, D., Mohammadnazari, Z., Aghsami, A., & Jolai, F. (2023). Factor identification for insurance pricing mechanism using data mining and multi criteria decision making. Journal of Ambient Intelligence and Humanized Computing, 14(7), 8153-8172. doi:10.1007/s12652-021-03585-z

Mamoudan, M. M., Jafari, A., Mohammadnazari, Z., Nasiri, M. M., & Yazdani, M. (2023). Hybrid machine learning-metaheuristic model for sustainable agri-food production and supply chain planning under water scarcity. Resources, Environment and Sustainability, 14, 100133. doi:https://doi.org/10.1016/j.resenv.2023.100133

Mantzana, V., Koumaditis, K., & Themistocleous, M. (2011). Healthcare IS interoperability: challenges and solutions. Paper presented at the International Conference on Health Informatics, HEALTHINF 2011.

Marino, C., Penedo, M. G., Penas, M., Carreira, M. J., & Gonzalez, F. (2006). Personal authentication using digital retinal images. Pattern Analysis and Applications, 9, 21-33.

Mason, J., Dave, R., Chatterjee, P., Graham-Allen, I., Esterline, A., & Roy, K. (2020). An investigation of biometric authentication in the healthcare environment. Array, 8, 100042.

Matloob, I., Khan, S., ur Rahman, H., & Hussain, F. (2020). Medical health benefit management system for real-time notification of fraud using historical medical records. Applied Sciences, 10(15), 5144.

Mousapour Mamoudan, M., Ostadi, A., Pourkhodabakhsh, N., Fathollahi-Fard, A. M., & Soleimani, F. (2023). Hybrid neural network-based metaheuristics for prediction of financial markets: a case study on global gold market. Journal of Computational Design and Engineering, 10(3), 1110-1125. doi:10.1093/jcde/qwad039

PK, R., Khaparde, A., Bendre, V., & Katti, J. (2024). Fraud detection and prevention by face recognition with and without mask for banking application. Multimedia Tools and Applications, 1-24.

Pourkhodabakhsh, N., Mamoudan, M. M., & Bozorgi-Amiri, A. (2023). Effective machine learning, Meta-heuristic algorithms and multi-criteria decision making to minimizing human resource turnover. Applied Intelligence, 53(12), 16309-16331. doi:10.1007/s10489-022-04294-6

Roh, J.-h., Cho, S., & Jin, S.-H. (2018). Learning based biometric key generation method using CNN and RNN. Paper presented at the 2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE).

Shakil, K. A., Zareen, F. J., Alam, M., & Jabin, S. (2020). BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. Journal of King Saud University-Computer and Information Sciences, 32(1), 57-64.

Srivastava, R., & Sharma, D. K. (2022). Human Authentication Using Score Level Fusion of Face and Palm Print Biometrics. In VLSI, Microwave and Wireless Technologies: Select Proceedings of ICVMWT 2021 (pp. 55-64): Springer.

Therar, H. M., Mohammed, L. D. E. A., & Ali, A. J. (2021). Multibiometric system for iris recognition based convolutional neural network and transfer learning. Paper presented at the IOP Conference Series: Materials Science and Engineering.

Umasankari, N., Muthukumar, B. and Shanmuganathan, C., 2024. Performance Evaluation of Biometric Authentication Using Fragment Jaya Optimizer-Based Deep CNN with Multi-kernel SVM. SN Computer Science, 5(4), p.337.

Vensila, C., & Boyed Wesley, A. (2024). Multimodal biometrics authentication using extreme learning machine with feature reduction by adaptive particle swarm optimization. The Visual Computer, 40(3), 1383-1394.

Venturini, L., Budd, S., Farruggia, A., Wright, R., Matthew, J., Day, T. G., . . . Hajnal, J. V. (2024). Whole-examination AI estimation of fetal biometrics from 20-week ultrasound scans. arXiv preprint arXiv:2401.01201.

Zafari, B., & Ekin, T. (2019). Topic modelling for medical prescription fraud and abuse detection. Journal of the Royal Statistical Society Series C: Applied Statistics, 68(3), 751-769.