Computer & Robotics

Presenting Multiple Biometric Identity Verification Model Based on Business Intelligence in Electronic Prescription System

Ahrar Hosseini [a] ,Reza Radfar [a,*] , Ataollah Abtahi [a]

[a] *Department of information technology management, science and research branch, Islamic azad university, Tehran, Iran*

Received 07 November 2023; Accepted 02 May 2024

Abstract

The healthcare industry confronts formidable challenges, prominently characterized by the imperative to optimize verification protocols for patient identities and medical records. This research highlights the importance of biometric authentication in ensuring secure and reliable identification with business intelligence. The proposed approach combines fingerprint and eye biometric features, leveraging the "or" relationship to authenticate individuals using either feature when necessary. By incorporating multiple biometric features, the model enhances accuracy and reliability, providing a comprehensive solution for identity verification. This study employs the Convolutional Neural Network (CNN) structure to process images for people authentication. The results of the proposed model demonstrate a 99% accuracy rate in correctly identifying individuals. The model's integration of multiple features and advanced machine learning techniques enhances authentication processes, enabling better management of access control and reducing unauthorized access risks. Future research should explore expanding the range of biometric features and further improving the model's architecture and algorithms to adapt to emerging technologies and security requirements. Overall, this research emphasizes the importance of biometric authentication, presents an effective approach, and paves the way for advancements in the field, enabling organizations to establish robust and secure identification systems.

Keywords: Multi-factor Authentication, Convolutional Neural Network, Image Processing, Fingerprint Authentication, Eye Biometrics Authentication

1.Introduction

Despite its special place and importance in every society, the large healthcare industry is still facing many challenges. There is a need to increase the speed and precision in all its activities because the delay in providing emergency medical services can endanger patients' lives or cause irreparable losses to individuals, hospitals, doctors, insurance companies [1]. One of the basic challenges in the healthcare industry that insurance organizations and medical centers are facing is the diagnosis and confirmation of patients' identities and their medical records for the use of medical services.

With the ever-increasing advancement of science and technology, the 21st century has witnessed the emergence of extensive innovations in the field of information technology, especially in healthcare systems. Using advanced technologies such as biometrics [2], blockchain [3], and artificial intelligence [4], studies have attempted to create robust systems to simplify the verification process to reduce costs for insurance organizations and improve the accuracy of treatment records. However, these systems require strong performance in data processing that can use different biometric characteristics of people in different situations. The combined biometrics presented in the studies developed for the purpose of identifying and authenticating people creates serious challenges.

The simultaneous use of several biometric features can also face many challenges [5]. For instance, when a system uses a combination of several biometric features, such as the biometric combination of fingerprint and signature scanning, if one of these biometric features is unavailable, it will not be possible to use this system.

The deployment of software and hardware to maintain data security, confidentiality, integrity, and data availability for such systems is very costly [6]. There are many problems in implementing these systems.

* Corresponding Author E-mail: r.radfar@srbiau.ac.ir

For example, the creation of electronic records has caused a significant increase in network traffic, software and hardware usage, as well as software attacks in healthcare organizations. This demonstrates the difficulty in finding a biometric feature that meets all requirements. The speed and accuracy of the biometric system must align with the system's requirements, not harm the users, be accepted by the target population, and provide sufficient protection against all kinds of security attacks.

To solve this challenge, there is a need for more innovative and advanced approaches that can be used in critical situations in addition to solving these challenges. For example, when a sober person enters a treatment center, using a national code or fingerprint can be the best way to identify him. Conversely, if an unconscious person or a person with compromised fingerprints enters the medical facility, or when one of the authentication systems does not show high accuracy, the designed system should still be able to recognize the person's identity. Therefore, this study suggests the combination of business intelligence in authentication methods.

This research highlights the importance of biometric authentication in ensuring secure and reliable identification in the health insurance industry. The proposed approach combines fingerprint and eye biometric features and uses the 'or' relationship to authenticate individuals using either feature when necessary. By combining multiple biometric features, this model increases accuracy and reliability, providing a comprehensive solution for identity verification in the health insurance industry. It is imperative to utilize several biometric models for authentication in the treatment sector. In the absence of a biometric index, alternative biometric authentication methods should be employed in the proposed system, along with the utilization of high-precision convolutional neural networks (CNNs) and effective processing of various image types. The results demonstrate remarkable performance with an accuracy rate of over 99% in fingerprint and eye biometric authentication. Integrating multiple features and advanced machine learning techniques into the model enhances authentication processes, enables better access control management, and reduces the risks of unauthorized access. Future research should explore expanding the range of biometric features and further improving model architectures and algorithms to adapt to emerging technologies and security requirements. Overall, this research emphasizes the importance of biometric authentication in the healthcare industry, providing an effective approach and paving the way for progress in this field, enabling organizations to implement robust identification systems and ensure safety.

The proposed approach can be used in all medical centers, and it establishes a fundamental link between patients and their medical records, which can lead to the reduction of fraud. Furthermore, this tool can be widely adopted, and its deployment cost is much lower compared to other systems.

To achieve the objectives mentioned above, the structure of this study is divided into sections. In the second part, relevant literature is reviewed, and the types of combined biometric systems are examined. The third part discusses the proposed model and the algorithm used for information processing. The fourth part examines the results of the proposed model. The fifth and sixth sections are dedicated to management approaches, model limitations, and future proposals, respectively. Finally, the seventh section presents the conclusion.

2. Literature Review

Smart healthcare, an emerging aspect of modern medical technologies, presents new challenges in data security, confidentiality, integrity, and availability. To address these challenges and ensure the security of medical data, biometric technology is considered an effective method and a key tool in maintaining data integrity and availability. Biometric systems offer significant opportunities for use in health systems, providing reliable security solutions and serving as authentication methods in various components of smart healthcare systems [7].

When individuals seek medical services at hospitals or clinics, different approaches can be employed to identify them and provide prompt care. In emergency situations where a person is unconscious or unresponsive, an authentication system that can identify individuals based on their biometric features enables healthcare professionals to quickly recognize the person and provide appropriate care. For instance, Manimekalai [8] proposed a healthcare system based on hybrid biometric authentication. Their model verifies the identity of an unconscious individual by scanning their fingerprint, face, or iris, while conscious individuals are asked to present their national identification card.

Research aimed to ensure efficient access to patients' health records for accurate medical services and privacy protection. Díaz-Palacios, Romo-Aledo and Chinaei [9] proposed the use of biometric systems to access a central health records database, safeguarding

patient privacy even in emergency cases. Their system utilizes a biometric terminal that employs mobile phone technology to transmit patient fingerprints from an emergency scene to a central database, enabling the retrieval of patient health record information while maintaining confidentiality in pre-hospital settings.

Mason, Dave [10] integrated eye biometrics and authentication processes in healthcare systems to establish secure patient identification. Their approach combines eye-related biometrics and patients' electronic indices within health information systems for identification purposes. Heidari and Chalechale [11] proposed a multimodal biometric scheme to enhance the authentication performance of healthcare systems and increase resistance against fraud. They employed deep learning techniques on a dataset of 1090 samples to authenticate individuals based on hand biometric features, including nails, fingerprints, and the ring, middle, and index fingers.

Alghamdi, Angelov and Alvaro [12] utilized deep learning techniques with different neural networks on biometric data associated with finger joints and nails to identify individuals. They introduced an automatic person recognition framework encompassing the localization of components in hand images, component detection and segmentation using bounding boxes, and similarity matching between two sets of segmented images. To further enhance data security and overcome limitations of unimodal biometric authentication, they employed a multimodal biometric authentication system and designed an authentication model based on integrated modeler diagrams [13].

In conclusion, biometric technology offers effective solutions to address the challenges of secure and reliable identification in smart healthcare systems. The integration of multiple biometric features, such as fingerprints, facial scans, iris scans, and eye-related biometrics, enhances accuracy and strengthens authentication processes. These advancements in biometric authentication contribute to improved patient care, privacy protection, and data security. Future research should continue to explore and refine multimodal biometric approaches to further enhance the performance and effectiveness of biometric authentication systems in healthcare.

In India, researchers conducted tests on various medical images in electronic health records, leading to the development of a biometric authentication system. Other studies focused on investigating the accuracy and implementation of combined biometric authentication systems. One approach involved combining fingerprint biometrics and facial recognition biometric systems for authentication purposes. The proposed system utilized fingerprint biometrics for authentication, encryption processes for confidentiality, and reversible watermarking for data integrity [14]. Another study proposed a multifaceted biometric authentication mechanism to reduce the misuse of health data and biometric patterns stored in heterogeneous cloud environments. They combined keystroke dynamics with facial recognition as a means of enhancing the system's accuracy in authenticating individuals [15].

Rohit et al. introduced a hybrid framework that applied principal component analysis and linear binary pattern to two biometric features, namely face and palm print, resulting in a unique score used for human authentication [16]. In 2017, a new multimodal biometric identification system was proposed, integrating facial biometrics, left iris, and right iris using deep learning approaches. The system employed a deep belief network architecture to define facial features and a combination of convolutional neural network and softmax classifier for iris recognition, extracting distinct features from iris images [17].

Shakil, Zareen [18] proposed a cloud-based healthcare data management system that ensured the security of electronic medical data access through signature scanning-based authentication. Neural networks were utilized to analyze the data, and the results demonstrated a significant improvement in test speed (9 times), with an error rate of 0.12, sensitivity of 0.98, and specificity of 0.95. In 2022, researchers presented a model for hybrid biometric authentication and patient privacy protection schemes in the healthcare system using blockchain technology. Their research indicated that this approach could create a natural barrier against data security-related problems [19]. Another study proposed a real-time decision support system that examined fingerprint data using a rule-based technique, with a focus on computational complexity and memory issues [20].

Ongoing research and advancements in biometric authentication in healthcare demonstrate the potential of integrating multiple biometric features and deep learning techniques to enhance accuracy, efficiency, and data security. Multimodal and hybrid biometric approaches are being utilized to overcome the limitations of unimodal systems, especially in healthcare and financial institutions. However, there is a need for innovative approaches that can be implemented practically and efficiently to address challenges in achieving high accuracy and speed in

identity verification systems. In the context of healthcare systems, accurate and rapid verification in the electronic prescription system, even with one unavailable biometric feature, is crucial. The integration of biometric systems with business intelligence can further enhance overall system performance, particularly in healthcare and treatment systems where patients may have specific issues. The proposed model combines multiple biometric features, such as scanning all fingers and iris scanning, either simultaneously or using the "OR" relationship, to increase speed and accuracy in identification. This approach considers factors like comprehensive database composition, effective biometric feature selection, and optimal combination methods. The subsequent sections will explore the relevant literature on the authentication approaches proposed in this study.

3. Methodology

The healthcare industry, despite its special place and importance in every society, faces numerous challenges that hinder its efficient operation. One critical challenge is the diagnosis and confirmation of patients' identities and their medical records for the use of medical services. The current processes employed by insurance organizations and medical centers to verify patient information are often time-consuming, error-prone, and costly. This not only poses a risk to patient safety, particularly in emergency situations where delays can be life-threatening, but also results in significant financial losses for individuals, hospitals, doctors, and insurance companies.

Additionally, the increasing reliance on information technology in healthcare systems has brought forth new opportunities and challenges. The emergence of biometric authentication systems holds promise in improving patient identification and record management. However, the effective implementation of such systems necessitates addressing several key challenges. Firstly, a comprehensive solution must be capable of utilizing different biometric features based on the situation, whether it is a sober patient entering a medical center or an unconscious individual requiring immediate care. This requires the ability to recognize and authenticate individuals accurately using a combination of available biometric features.

Furthermore, deploying biometric systems in healthcare organizations entails addressing significant concerns regarding data security, confidentiality, integrity, and availability. The introduction of electronic medical records has led to increased network traffic, software and hardware usage, and susceptibility to software attacks, posing a threat to the overall security of healthcare organizations. Thus, developing a robust and cost-effective biometric system that meets the requirements of speed, accuracy, user acceptance, and protection against security threats becomes crucial.

In light of these challenges, this study aims to design a system for authenticating individuals by combining biometric systems with business intelligence. By leveraging the relationship between different biometric features, the proposed model seeks to enhance system performance and accuracy. The effectiveness of the model will be evaluated through the use of a convolutional neural network to process and analyze data from each biometric feature. The study expects the proposed approach to be applicable across various medical centers, establishing a reliable connection between patients and their medical records while minimizing the risks of fraud. Additionally, the deployment cost of this system is anticipated to be lower compared to alternative solutions. To address this issue, in this section of the study, we will outline the relevant methodology.

3.1. Problem Description

According to the aforementioned information, this study proposes the utilization of multiple biometric features, such as fingerprint scanning, iris scanning, and face scanning, in a combined manner using the logical "OR" relationship. This approach ensures that if one biometric feature is unavailable or a scanner malfunctions, other registered features can be used for identity verification and accessing medical records.

In this system, the model initially employs fingerprint scanning for identity confirmation. If fingerprint scanning fails, the alternative method of iris scanning is used. If neither fingerprint nor iris scanning confirms the identity, the system proceeds to use face scanning. Additionally, this system can incorporate several other biometric methods for identity verification. This proposed model is a fusion of biometric systems and business intelligence, enhancing the speed and accuracy of identity recognition by seamlessly transitioning between different identification methods in the absence of any specific feature. To establish the proposed system, several crucial factors have been examined, including consolidating databases related to each feature into a single data warehouse, selecting the most suitable biometric features for the multi-biometric system, and

designing an optimal method for combining biometric features to verify individuals' identities.

The process of biometric identification commences with capturing and recording individuals' fundamental physical characteristics. Depending on the type of biometric method employed, such as physiological or behavioral data, specific details of these characteristics are obtained and stored in a specialized format within the system. Contrary to popular belief, the system does not store the entirety of the collected information, such as fingerprints or face scans. Instead, registration algorithms extract key features during the registration and scanning process, forming a general template. Each biometric system possesses its own registration algorithms, and these templates can be stored locally on a PC or network server.

The biometric authentication system for identification encompasses three main stages: biometric feature scanning, feature extraction, and verification and pattern matching. During the first stage, sensors and scanners capture and record individuals' biometric characteristics. In the second stage, biometric features are extracted from the recorded input data. Finally, the model validates the data by identifying the biometric pattern and makes the final decision to accept or reject the individual's identity. Figure 1 illustrates the general structure of this study, incorporating the core architecture of the fingerprint recognition system, business intelligence, and a real-time cache and warning system. The proposed model adopts a layered architecture consisting of the operational layer, data warehouse, data analysis layer, and report layer.

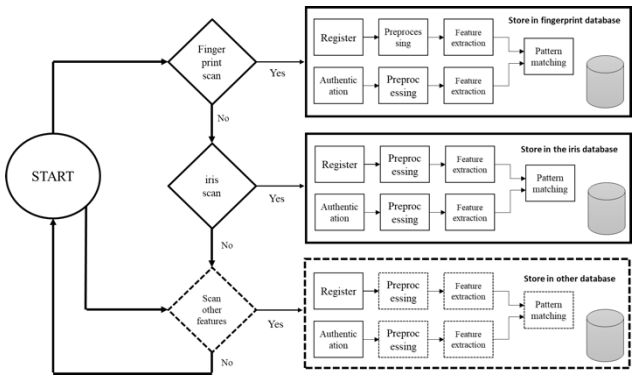

Fig. 1. general structure of this study

The operational layer acts as the communication point between the sensor receiving the biometric feature and the corresponding databases for each biometric feature. This communication point supplies input to the data warehouse, which is periodically updated as data is entered from the local database. The analysis layer utilizes classification, a data mining technique, to analyze the data. Classification involves discovering hidden knowledge, patterns, and relationships within extensive datasets using mathematical techniques such as decision trees, linear programming, neural networks, and statistics. By learning from past experiences, the analysis layer identifies the most effective model for describing data concepts and classes.

In the proposed model, the report layer receives data through the communication port, where the sensor captures biometric features, processes the user-provided information, and sends it to the server to confirm or reject the person's identity. Valid identification information is then transferred to the data warehouse, which serves as the repository for all features and queries, regularly updating its stored data. The analysis layer continuously analyzes the data generated by the data warehouse. Finally, the report layer presents the requested and real-time reports based on the knowledge and information stored in the analysis layer. Overall, this study proposes the utilization of multiple biometric features in combination with business intelligence, employing a layered architecture to enhance system performance, accuracy, and reporting capabilities.

3.2. Data Description

In this section, our objective is to provide a comprehensive description of the data used in our study. We aim to present a detailed analysis and characterization of the datasets employed, highlighting their key features and properties. By delving into the specifics of the data, we can gain a deeper understanding of its composition and structure, laying the foundation for further analysis and interpretation. Through meticulous examination and explanation, we aim to provide a clear and concise depiction of the data, enabling readers to grasp its significance and relevance to our research.

This model suggests using fingerprint biometrics as the initial method for authentication. If there are issues with the finger area or the scanner, the system can utilize other biometric features. The dataset used is called B_DB4_FVC2000, which contains fingerprint information from ten individuals. Each person has eight fingerprint photos, resulting in a total of 80 photos. To enhance the dataset, data augmentation techniques are employed to create

manipulated versions of existing images, generating 72 new fingerprint photos per person. This technique helps the network learn new features and improve generalization. The dataset includes 600 fingerprint images from individuals in Africa, with gender and hand-specific tags. The images have a resolution of 1 x 96 x 103 and are available for non-commercial research purposes. Labels in the file provide information about each image, including sample number, gender, hand, finger name, data augmentation technique, and file extension.

In cases where fingerprint authentication is not feasible, this study proposes using iris recognition as an alternative. The dataset employed for this purpose is called V1_UBIRIS, comprising 1877 eye photos from 241 individuals. The eyes in the images are first identified using Har's waterfall algorithm, and then the irises are isolated. Image processing tools and a convolutional neural network are utilized to classify the data. During the registration process, patients' biometric information is collected through sensors and imaging tools, and the registered image samples are trained using the proposed neural network.

3.3. Authenticating Proposed Approach

Convolutional Neural Networks (CNNs) can be characterized as advanced neural networks that possess deep architectures [21]. CNNs consist of five distinct layers: the input layer, convolution layer, pooling layer, fully connected layer, and output layer [22]. In the output layer, the received properties are processed to generate the desired outputs. The structure of a CNN, as depicted in Equation 1, represents the calculation formula used for CNNs [23]. In this equation, the output size is denoted by N, the input size is represented by W, the convolution kernel size is denoted by F, the padding value size is indicated by P, and the step size is represented by S.

$$N = (W - F - 2P)/S + 1 \quad [1]$$

The convolution layer plays a crucial role in extracting features from the input data [24]. Generally, it comprises the convolution kernel, convolutional layer parameters, and an activation function. This layer holds significant importance within the CNN architecture. By utilizing convolution kernels, the convolution layer extracts features from the input variables, thereby capturing the essence of property extraction. The size of the convolution kernels is smaller than that of the input matrix. Instead of conventional matrix operations, the convolution layer employs convolution operations to generate the feature map. The computation of each element in the feature map follows Equation 2. In Equation 2, $x_{i.j}^{out}$ represents the output value at row i and column j of the feature map, $x_{i+m,j+n}^{in}$represents the value at row i and column j of the input matrix, $f_{cov}(0)$ denotes the chosen activation function, $w_{m,n}$signifies the weight at row m and column n for the convolution kernel, and b represents the bias of the convolution kernel [25].

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

Generally, in the convolution layer of a CNN, multiple kernels are used with the input matrix. Each kernel extracts a feature from the input matrix, resulting in a feature map. The pooling layer then reduces the dimensions of the feature map, enhancing computational efficiency through down-sampling. The pooling layer also helps in reducing the output of feature vectors generated by the convolutional layer while improving the overall results. CNN demonstrates a strong capability in extracting features from grid data, expanding m variables of any type to n stations and forming an m-row by n-column matrix. In terms of CNN's structure, the fully connected layer serves as a classifier, positioned at the end of the network. It performs regression classification on the extracted features. Therefore, CNN can be divided into two parts: the first part involves feature extraction (convolution, activation function, pooling), and the second part focuses on classification and recognition (fully connected layer).

3.3.1. Model Training

The convolutional neural network has been chosen as the algorithm proposed for data classification in this study's model. This network learns from a given dataset to classify the data into appropriate groups with minimal error.

In the process of classifying data using different models, the dataset is divided into two categories: training data and testing data. Typically, 80% of the dataset is selected as training data, while the remaining 20% is used for testing. The remaining data is reserved for testing and validation purposes. Essentially, the designed system learns the function of the training data and evaluates its accuracy by testing it on the test data for data classification.

Once the training process is completed, it is crucial to evaluate the trained model. It is important to note that the evaluation of the trained network has been performed using the test data.

3.3.2. Model Evaluation

Accuracy is a fundamental metric for assessing classification models, including convolutional neural networks (CNNs). It measures the proportion of correctly classified instances compared to the total number of instances in the dataset, reflecting how well the model predicts the correct class labels. Typically evaluated on a separate test dataset, accuracy alone may not provide a complete picture, especially with imbalanced data or varying costs of misclassification [26]. Additional metrics like precision, recall, and F1-score offer a more comprehensive evaluation. It's important to interpret accuracy within the specific context, considering other factors and metrics to ensure the model's suitability. Regular monitoring and evaluation of accuracy, along with other performance metrics, help identify areas for improvement and guide enhancements in the classification model. Equation 3 shows the Accuracy formulation. In the Equation 3, T_p related to True Positive. T_N related to True Negative. F_p shows False Positive and F_N shows False Negative.

$$\text{Accuracy} = \frac{T_p + T_N}{T_p + T_N + F_p + F_N} \quad [3]$$

Precision is a crucial metric used to evaluate the performance of classification models, particularly when minimizing false positives is important. It measures the proportion of correctly predicted positive instances out of all instances predicted as positive by the model. By assessing precision, we can determine the model's ability to accurately identify true positive instances while reducing false positives. A higher precision value indicates a lower rate of misclassifying negative instances as positive. Precision is especially valuable in scenarios where false positives carry significant consequences or costs, such as in medical diagnosis. However, precision should be considered alongside other metrics like recall and accuracy to gain a comprehensive understanding of the model's performance. There may be a trade-off between precision and recall, where improving one might result in a decrease in the other. Selecting the appropriate evaluation metric depends on the specific goals of the classification task. Regular monitoring and evaluation of precision enable optimization of the model's performance and enhance its reliability in real-world applications. The Equation 4 shows the precision formulation. In this Equation T_p shows True Positive and F_p shows False Positive.

$$Precision = \frac{T_p}{T_p + F_p} \quad [4]$$

Recall, also known as sensitivity or true positive rate, is a critical metric in assessing classification model performance, specifically when minimizing false negatives is important. It measures the proportion of correctly predicted positive instances out of all actual positive instances. A higher recall value indicates a lower rate of misclassifying positive instances as negative. This metric is particularly valuable in scenarios where missing positive instances can have significant consequences or costs. However, it should be considered alongside other evaluation metrics like precision and accuracy to obtain a comprehensive understanding of the model's performance. Regular monitoring and evaluation of recall can help refine the model, ensuring its reliability and effectiveness in real-world applications. The Equation 5 shows the Recall formulation. In this Equation T_p shows True Positive and F_n shows False Negative.

$$Recall = \frac{T_p}{T_p + F_n} \quad [5]$$

The F1 score is a widely used evaluation metric that combines precision and recall into a single value, providing a balanced measure of a model's performance. It represents the harmonic mean of precision and recall, ranging from 0 to 1. The F1 score is particularly valuable when achieving both high precision and high recall is important, such as in imbalanced class distributions or when false positives and false negatives have significant consequences. A high F1 score indicates a model's effectiveness in accurately classifying positive instances while minimizing false negatives and false positives. Optimizing the F1 score helps improve overall model performance, and regular monitoring aids in identifying areas for enhancement. By aiming for a high F1 score, practitioners can develop more reliable and effective classification models for diverse applications. The Equation 6 shows the F1 score formulation.

$$F1\ score = \frac{2 \times precision \times recall}{precision + recall} \quad [6]$$

4. Result and Discussion

A comprehensive approach is taken in this study to develop a convolutional neural network (CNN) architecture for authenticating individuals using eye and fingerprint biometric features. The network incorporates an "or" relationship between biometric features, allowing seamless authentication even when certain features are unavailable. Emphasis is placed on maximizing the accuracy of each biometric feature to ensure the efficiency and effectiveness of the proposed system. Performance evaluation criteria, including accuracy, coverage, and F1- Score, are used to assess the model's accuracy and effectiveness. The results demonstrate the system's ability to authenticate individuals using various biometric features, highlighting the potential of the proposed model. This study contributes to the development of biometric authentication systems and has implications for applications such as access control and identity verification. Further research and improvements in individual biometric feature accuracy can lead to stronger and more reliable authentication systems in the future. The results of the tests, which demonstrate the effectiveness of the convolutional neural network approach in the authentication process, are presented in Table 1.

Table 1
The Use of Convolutional Neural Network in Fingerprint Biometrics

	Accuracy	Precision	Recall	F1 Score
Fingerprint Biometrics	0.9945878	0.9949353	0.9945878	0.9945830

Table 1 provides compelling evidence of the remarkable performance of the proposed model in authenticating individuals using fingerprints. The results clearly indicate that the model achieved an impressive accuracy of 0.9945878 in accurately identifying individuals' identities, as measured by the accuracy criterion. This high level of accuracy underscores the effectiveness of the proposed model in precisely identifying people based on their fingerprint biometric features.

Furthermore, the proposed model demonstrates commendable accuracy of 0.9949, as indicated by the accuracy criterion. This reinforces the reliability and robustness of the model in accurately verifying the identity of individuals. Additionally, the coverage measures and F1 measure offer valuable insights into the model's performance. With coverage values equal to 0.9945878 and an F1 criterion value of 0.9945830, this model showcases its ability to effectively encompass a broad range of individuals while maintaining a balanced precision and recall trade-off. To visually demonstrate the accuracy of the proposed model in fingerprint authentication, Figure 2 illustrates the accuracy graph. The red lines represent the training data, while the blue lines depict the test data. This graph provides a visual representation of the model's performance, showcasing its consistent high accuracy on both the training and test data sets. The convergence and stability of the accuracy lines further signify the model's robustness and reliability in fingerprint-based authentication.

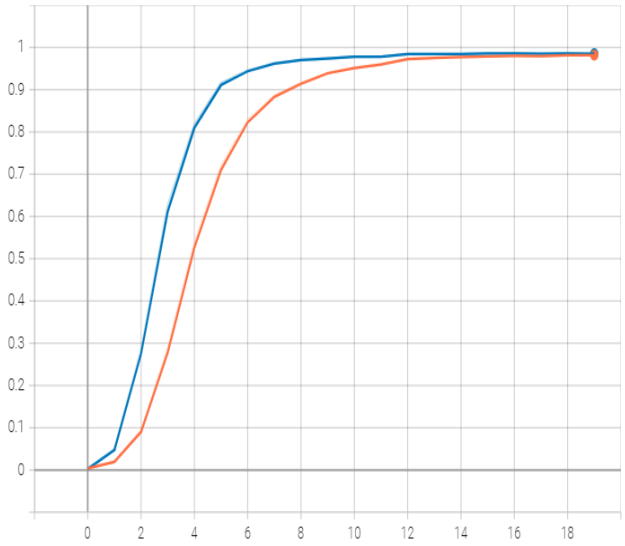

Fig. 2. Fingerprint Authentication Accuracy

The results presented in Table 1 and Figure 2 highlight the effectiveness of the proposed model in fingerprint authentication. The noteworthy accuracy scores and convergence depicted in the accuracy graph underscore the potential and dependability of the model in accurately verifying individuals' identities using fingerprint biometric features. These findings contribute to the advancement of biometric authentication systems and underscore the viability of fingerprint-based authentication in various applications requiring secure and reliable identification. Further research and exploration of diverse biometric features hold the potential to expand the scope and effectiveness of the proposed model, opening doors to advanced biometric authentication systems in the future.

In addition to accuracy analysis, the loss function provides valuable insights into the performance and suitability of the proposed model for fingerprint

authentication. Figure 3 illustrates the loss function specifically designed for this purpose. The loss function serves as a measure to evaluate the model's capability and its ability to make accurate predictions on new fingerprint data. It quantifies the discrepancy between the actual and predicted results, representing the error rate of the neural network during training.

The loss function plays a vital role in the neural network training process. By utilizing a loss function, the model's weight values are continuously adjusted, enabling the network to iteratively improve its predictions and strive for better accuracy. As training progresses, the loss function provides crucial feedback on the model's performance, guiding the optimization process to minimize errors and enhance overall prediction accuracy.

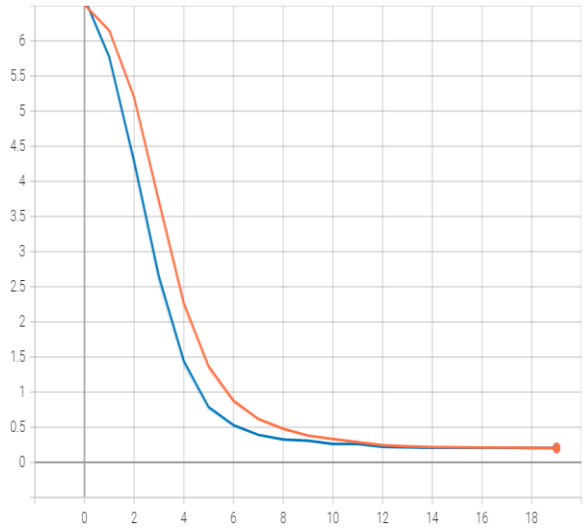

Fig. 3. Fingerprint Authentication Loss Function

Figure 3 presents a visual representation of the loss function's performance in the context of fingerprint authentication. The plot showcases the behavior of the loss function for both the training data (red lines) and the test data (blue lines). This plot provides insights into the convergence and stability of the loss function, indicating the model's ability to continually learn and adapt to the training data while maintaining satisfactory performance on unseen test data.

The analysis of the loss function, as depicted in Figure 3, aids in understanding the model's performance and its capacity to accurately predict new fingerprint data. By minimizing the loss function's value, the proposed model continuously enhances its predictive capabilities, enabling reliable and accurate fingerprint authentication. These findings reinforce the effectiveness and appropriateness of the proposed model, laying a solid foundation for the development and implementation of robust fingerprint-based authentication systems.

After analyzing Table 1, the proposed model demonstrates exceptional performance across different evaluation criteria. Regarding accuracy, the model achieves an impressive value of 0.9949353, indicating its ability to accurately predict subsequent fingerprint data with over 99% accuracy. This highlights the reliability and effectiveness of the model in identifying individuals based on their fingerprints.

Additionally, when considering the coverage criterion, the proposed model maintains a high level of accuracy with a value of 0.9945878. This signifies the model's reliable 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 measure of precision and reliability, reaffirming the model's ability to achieve high precision and recall in accurately verifying the identity of individuals based on their fingerprints.

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

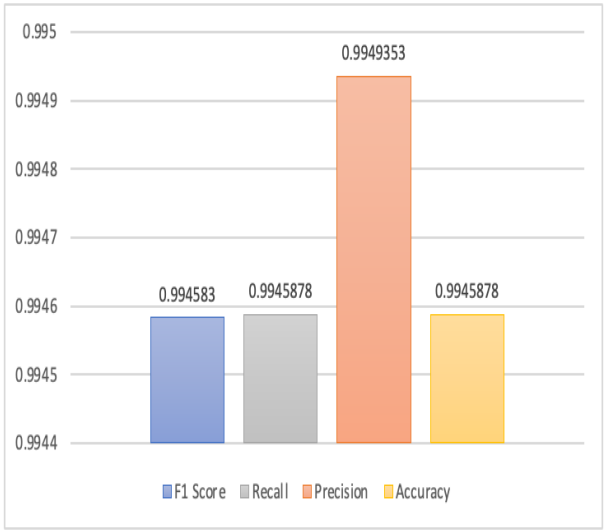

Fig. 4. Performance of Convolutional Neural Network in Fingerprint Authentication

In summary, the results from Table 1 and the accompanying graph in Figure 4 demonstrate the strength and accuracy of the proposed model in predicting and verifying the identity of individuals based on their fingerprints. The high values obtained in the evaluation criteria affirm the effectiveness of the model and establish it as a reliable solution for fingerprint-based authentication systems.

The results presented in Figure 4 provide compelling evidence regarding the effectiveness and accuracy of the proposed model in fingerprint authentication. Across all evaluation criteria, the model consistently achieves an accuracy rate exceeding 99%, demonstrating its high validity and robust performance. This exceptional accuracy reaffirms the model's capability to precisely identify and authenticate individuals based on their unique fingerprint patterns.

Furthermore, Figure 5 offers a visualization of the network structure employed in the proposed model for fingerprint authentication. This graphical representation provides insights into the architectural design, showcasing the interconnected layers and nodes that collectively contribute to accurate identification. Understanding the structure of the network enables researchers and practitioners to delve deeper into the underlying mechanisms and algorithms utilized, fostering transparency and reproducibility.

To summarize, the combination of evidence from Figure 4 and Figure 5 underscores the remarkable accuracy, reliability, and robustness of the proposed model for fingerprint authentication. Consistently high accuracy rates across various evaluation criteria validate the model's performance and establish it as a suitable and effective solution for precise and dependable identification based on fingerprints. The visual representation of the network structure augments our understanding of the model's inner workings, empowering researchers and practitioners to enhance its overall performance.

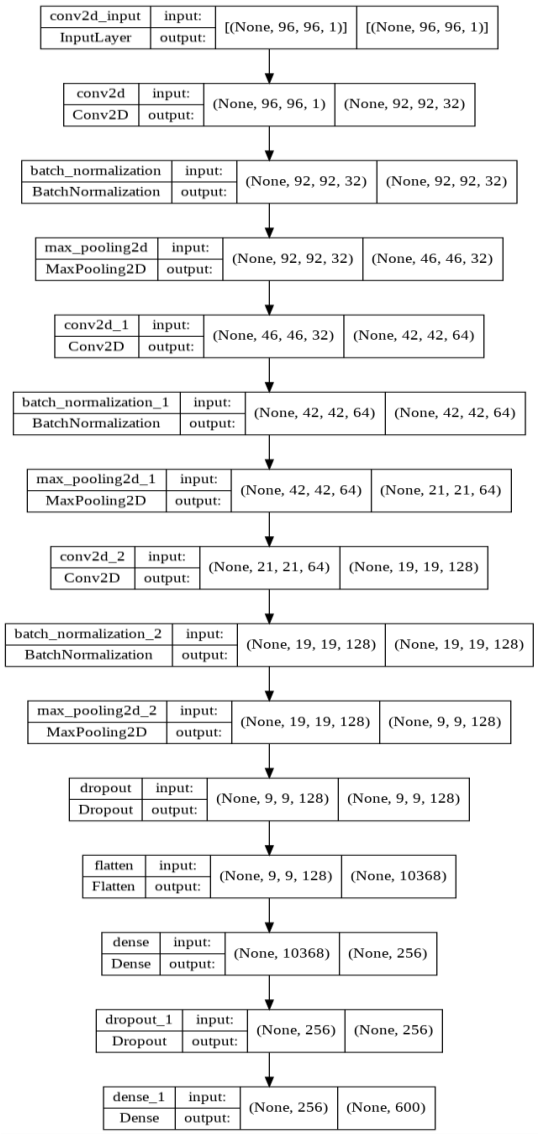

Fig. 5. Proposed Network Structure in Fingerprint Authentication

The proposed model demonstrates flexibility by utilizing alternative biometric features when the primary feature is unavailable. Maintaining high accuracy across all considered biometric features is crucial to ensure effective verification or denial of individuals' identities using any available feature. For instance, in cases where fingerprint data is inaccessible due to injuries or damage, healthcare facilities can rely on other features such as eye scans for identification.

In this study, the proposed model addresses this requirement by suggesting the use of the eye biometric feature as an alternative when fingerprint data is not applicable. The accuracy of each biometric feature is significantly enhanced to maximize their effectiveness in identifying individuals. By combining multiple biometric features and improving

their accuracy, the proposed model ensures that even in situations where primary features are unusable, an alternative feature can successfully authenticate individuals and maintain system efficiency.

Table 2 presents the results obtained from applying a convolutional neural network to eye biometrics. These results showcase the model's performance in accurately detecting and authenticating individuals based on their eye features. The table provides comprehensive information about the model's accuracy and confirms its suitability for precise and robust identification using eye biometric data.

Table 2
The Use of Convolutional Neural Network in Eye Biometrics

	Accuracy	Precision	Recall	F1 Score
Eye Biometrics	0.9965	0.9960101	0.9965	0.996373

The results obtained, as shown in Table 2, highlight the exceptional performance of the proposed model in authenticating individuals based on eye biometric features. With an accuracy criterion of 0.9965, the model demonstrates a significant ability to accurately identify and verify people's identities. This high level of accuracy ensures reliable confirmation or denial of individuals' identities using eye biometric data.

To visually represent the model's accuracy, Figure 6 displays a graph illustrating the accuracy values of the proposed model using the eye biometric feature. The red lines represent the test data, while the blue lines correspond to the training data. This graph provides a clear understanding of accuracy trends and reinforces the consistent and reliable performance of the proposed model in using eye biometrics for identification purposes.

Overall, the presented table and graph confirm the effectiveness of the proposed model in accurately recognizing individuals based on their eye biometric features, highlighting its potential to enhance identity verification systems across various domains.

In addition, Figures 7 offer insights into the loss performance associated with the authentication process using the eye biometric feature. Similar to fingerprint biometrics, the loss function serves as a measure to evaluate the model's skill and its ability to accurately predict new data. By quantifying the difference between actual and predicted results, the loss function guides the network towards improved and more accurate solutions by updating the weights.

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 reveals the fluctuations of the loss function in successive iterations, indicating the optimization process of the model. The ultimate goal is to minimize the loss function and approach a value close to zero, indicating high accuracy and robustness in authentication using eye biometric features.

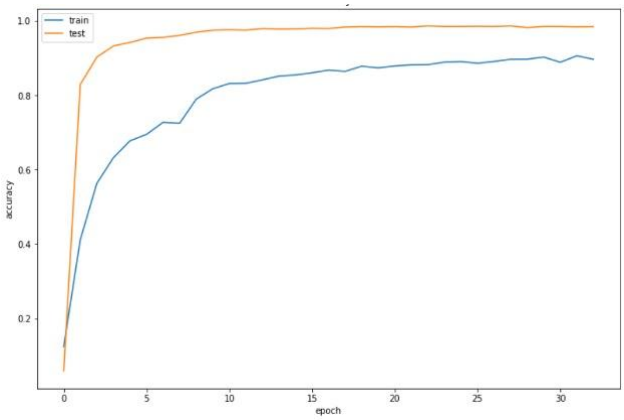

Fig. 6. Eye Biometrics Authentication Accuracy

These visual representations, both the accuracy graph (Figure 6) and the loss function graph (Figure 7), complement the quantitative results presented in the table and provide a comprehensive understanding of the performance and optimization process of the proposed model in eye biometric authentication. They further confirm the effectiveness and reliability of the proposed approach in accurately verifying people's identities using their eye features.

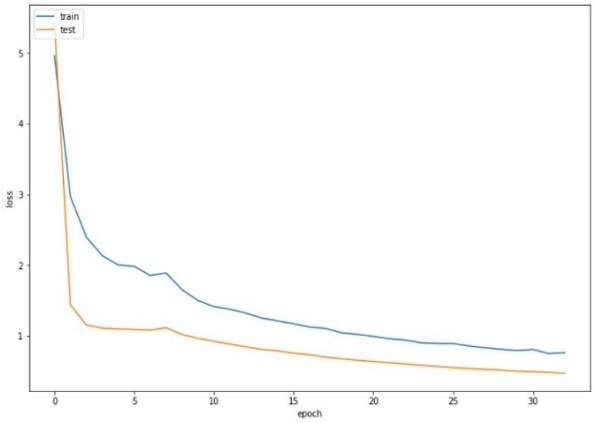

Fig. 7. Eye Biometrics Authentication Loss Function

As evident from Table 2, the proposed model for authentication using eye biometric features demonstrates significant accuracy values. With an accuracy criterion score of 0.9960101, the model exhibits the ability to correctly recognize the identity of individuals in the eye biometrics dataset. Similarly,

the coverage measure indicates an accuracy of 0.9965, implying the model's ability to predict subsequent data with an accuracy rate exceeding 99%.

Moreover, the F1 criterion value of 0.9963273 highlights the overall performance of the model considering precision and recall criteria. These remarkable results affirm the effectiveness and reliability of the proposed model in utilizing eye biometric features for identity verification.

To provide a visual representation of the model's performance in different evaluation criteria, Figure 8 presents a graph illustrating its performance. This graph offers insights into accuracy, coverage, and F1 scores, enabling a comprehensive assessment of the model's overall performance.

Together, these quantitative findings and visual representations demonstrate the robustness and high performance of the proposed model in authenticating individuals using eye biometric features. The results emphasize the significance of combining multiple biometric features to ensure accurate identity verification, even in scenarios where one feature may not be available or applicable.

In fact, Figure 8 provides an overview of the evaluation criteria in the authentication process using eye biometric features. This graph shows the accuracy, coverage and F1 criterion values, all of which exceed the 99% threshold, indicating the model's ability to accurately confirm or reject the identity of individuals. This strengthens the reliability and effectiveness of the proposed model in the authentication process.

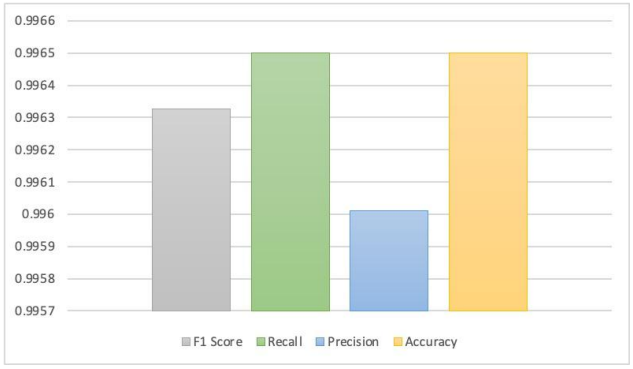

Fig. 8. Performance of Convolutional Neural Network in Eye Biometrics Authentication

In addition, Figure 9 shows the network structure of the proposed model, which is specifically designed to authenticate people using eye biometric features. This visual representation allows a better understanding of the underlying architecture and information flow within the model. It provides insight into the sequence of layers, connections, and computational processes involved in the authentication process.

By combining advanced technologies such as convolutional neural networks and using eye biometric features, the proposed model shows its potential in achieving highly accurate and reliable identity verification. The combination of robust evaluation criteria and well-designed network structure ensures the efficiency and effectiveness of the model in real-world applications.

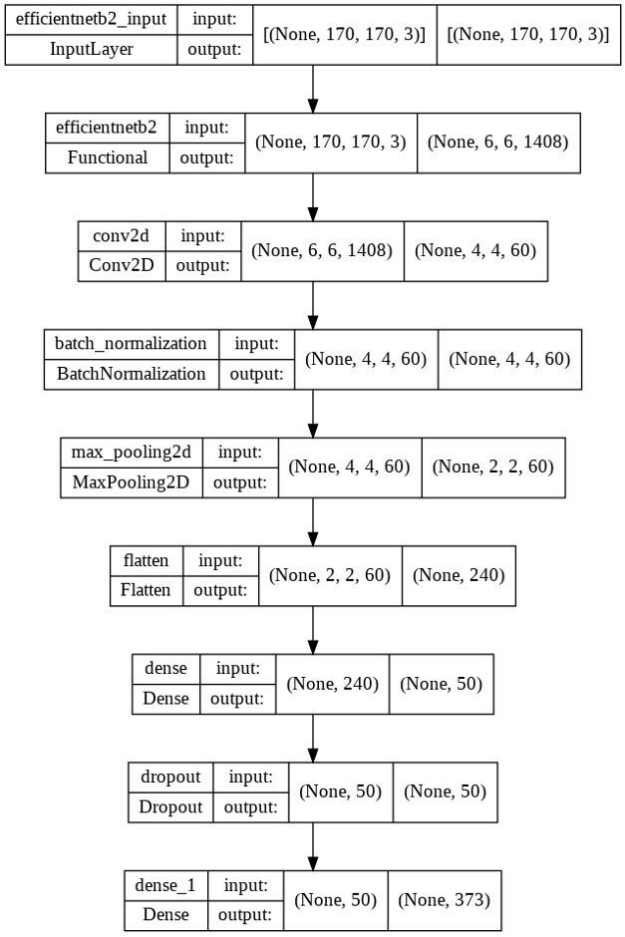

Fig. 9. Proposed Network Structure in Eye Biometrics Authentication

5. Managerial Insight

The development of a robust convolutional neural network model for biometric authentication presents significant managerial insights. By considering the "or" relationship between biometric features, this model offers flexibility and adaptability in situations where certain features may not be available or feasible for authentication. This insight allows managers to implement authentication systems that can seamlessly switch between different biometric features, ensuring

uninterrupted access while maintaining a high level of security.

One key managerial application of this model lies in access control systems. Organizations can deploy this model to enhance security measures by integrating eye and fingerprint biometric authentication. This provides a reliable and efficient means of granting access to restricted areas, secure buildings, and sensitive facilities. By leveraging this model, managers can ensure that only authorized individuals with verified biometric features can gain entry, reducing the risk of unauthorized access and potential security breaches.

Another important application is in the realm of secure transactions. In today's digital landscape, ensuring the security of online transactions is paramount by incorporating this model into online banking, e-commerce platforms, and digital payment systems, managers can enhance the authentication process. Users can be reliably identified based on their eye and fingerprint biometric features, reducing the risk of fraudulent activities and unauthorized access. This managerial insight not only protects users' financial interests but also safeguards the reputation and integrity of the organization.

Identity verification is another area where this model can be effectively employed. Government agencies, immigration departments, and law enforcement organizations can utilize this model to verify individuals' identities. By authenticating individuals using their eye and fingerprint biometric features, managers can enhance the accuracy and reliability of identity verification processes. This insight contributes to improved border control, issuance of identification documents, and more effective criminal investigations.

Moreover, the managerial insight provided by this model extends to employee attendance and time tracking systems. Organizations can implement this model to ensure accurate identification and recording of employee presence. By relying on eye and fingerprint biometric authentication, managers can prevent time theft, eliminate buddy punching, and enhance payroll accuracy. This insight contributes to improved workforce management, increased productivity, and cost savings for the organization.

Additionally, healthcare systems can benefit from implementing this model for secure patient identification and access control. By incorporating eye and fingerprint biometric authentication, managers can safeguard patient records, control access to medical information, and prevent unauthorized entry to healthcare facilities. This managerial insight ensures data privacy, reduces the risk of medical identity theft, and enhances overall patient safety and care quality.

In summary, the managerial insight provided by this model emphasizes the importance of flexible and robust biometric authentication systems. Managers can leverage this model in various domains, including access control, secure transactions, identity verification, employee attendance, mobile device security, and healthcare systems. By adopting this model, managers can enhance security, improve efficiency, mitigate risks, and ensure compliance with regulatory requirements. Understanding the applications and managerial implications of this model empowers decision-makers to implement effective and reliable biometric authentication solutions tailored to their organizational needs.

6. Limitation and Feature Study

While the proposed convolutional neural network model for biometric authentication offers valuable insights and applications, it is important to acknowledge its limitations and identify areas for future research. Understanding these limitations and addressing them through further studies can enhance the model's effectiveness and broaden its applicability.

One potential limitation of the model lies in the reliance on specific biometric features such as eye and fingerprint data. Further research is needed to explore the integration of additional biometric modalities, such as voice recognition, facial recognition, or behavioral biometrics. Investigating the combination of multiple biometric features can lead to more robust and accurate authentication systems, enhancing both security and user experience.

Another avenue for future research is the exploration of the model's performance in diverse demographic groups. Biometric features can vary across different populations, and it is essential to evaluate the model's accuracy and reliability in various ethnicities, ages, and genders. Assessing the model's effectiveness in accommodating demographic variations can ensure inclusivity and minimize biases in the authentication process.

Furthermore, the model's performance in real-world scenarios and under varying environmental conditions should be investigated. Factors such as lighting conditions, image quality, and sensor accuracy can impact the reliability of biometric data capture. Conducting studies that evaluate the model's performance in different environments and under

challenging conditions can provide valuable insights into its practical applicability and identify areas for improvement.

An important research question is the model's vulnerability to spoofing attacks or presentation attacks. Evaluating the model's resilience against fake or manipulated biometric data can help identify potential security risks and develop countermeasures to enhance the system's robustness. Exploring anti-spoofing techniques and studying the model's response to different attack scenarios are crucial areas of investigation.

Additionally, the usability and user acceptance of the model should be studied. User experience, user interface design, and user perception of the authentication process can impact the adoption and effectiveness of the system. Investigating users' attitudes, preferences, and concerns regarding the biometric authentication process can provide insights for designing more user-friendly and trusted systems.

Finally, the model's scalability and computational efficiency should be addressed. As the size of the dataset and the number of users increase, it is important to assess the model's scalability and its ability to handle a large volume of biometric data. Optimizing the model's architecture and exploring parallel processing techniques can help improve its efficiency and reduce computational requirements.

In conclusion, further research is needed to overcome the limitations and advance the features of the proposed convolutional neural network model for biometric authentication. Exploring the integration of additional biometric modalities, studying the model's performance in diverse populations and environmental conditions, evaluating its resilience against spoofing attacks, investigating user acceptance, and optimizing scalability and computational efficiency are important areas for future research. Addressing these research questions will contribute to the development of more robust, accurate, and practical biometric authentication systems.

7. Conclusion

The research underscored the critical role of biometric authentication in ensuring secure identification across various domains. With advancing technology, the demand for precise and efficient biometric authentication systems became increasingly significant. The study proposed an innovative approach that integrated fingerprint and eye biometric features, capitalizing on their combined strengths for identity verification. By leveraging an "or" relationship, the system could authenticate individuals using either biometric data, ensuring accurate identification even when one feature was unavailable or unsuitable. This approach enhanced the accuracy and reliability of the model, offering a comprehensive solution for identity verification.

A convolutional neural network (CNN) was employed to achieve high accuracy and effectively process diverse image types. CNNs were well-suited for image recognition tasks due to their ability to discern complex patterns and features from data. The study demonstrated the CNN's proficiency in accurately analyzing fingerprint and eye images, facilitating precise identification and verification of individuals. Remarkable performance was observed in both fingerprint and eye biometric authentication, with the proposed model consistently surpassing 99% accuracy rates, affirming its reliability and effectiveness in recognizing and authenticating individuals based on biometric features. The proposed model presented a practical management solution for organizations reliant on secure identification systems. By integrating multiple biometric features and employing advanced machine learning techniques, the model enhanced authentication accuracy and efficiency, thereby improving access control management and mitigating the risk of unauthorized access.

Future research avenues should explore incorporating additional biometric modalities, such as voice or facial recognition, to further enhance the model's comprehensiveness and accuracy. Continuous refinement of the model's architecture and algorithms would bolster its adaptability to emerging technologies and evolving security needs, paving the way for advancements in biometric authentication systems.

Author Contributions: All authors collaborated on the study's conception and design. Ahra Hosseini, Reza Radfar, and Ataollah Abtahi were responsible for tasks such as material preparation, data collection, and analysis. Ahra Hosseini initially drafted the manuscript, incorporating input from all authors during the review of previous versions. The final manuscript received unanimous approval from all authors. Ahra Hosseini contributed to conceptualization, writing, methodology, and software implementation, while Reza Radfar and Ataollah Abtahi provided oversight in terms of supervision, project administration, review, and editing. All authors have read and approved the published manuscript.

Data Availability and Access: Due to the nature of this research, the study participants did not provide consent for public data sharing. Therefore, supplementary data is not available for public distribution.

Conflict of Interest: The authors declare no conflicts of interest.

Ethical and Informed Consent for Data Usage: Not applicable.

Funding: This research did not receive external funding.

Institutional Review Board Statement: Not applicable.

References

[1]. Mamoudan, M.M., et al., *Factor identification for insurance pricing mechanism using data mining and multi criteria decision making.* Journal of Ambient Intelligence and Humanized Computing, 2023. **14**(7): p. 8153-8172.

[2]. Li, N., et al., *Deep‐Learning‐Assisted Thermogalvanic Hydrogel E‐Skin for Self‐Powered Signature Recognition and Biometric Authentication.* Advanced Functional Materials, 2024: p. 2314419.

[3]. Rezvani, M. and H. Khani, *E-voting over blockchain platforms: A survey*. Journal of Network Security and Data Mining, 2019. **2**(3): p. 1-14.

[4]. Olabanji, S.O., et al., *AI for Identity and Access Management (IAM) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorization, and access control within cloud-based systems.* Authorization, and Access Control within Cloud-Based Systems (January 25, 2024), 2024.

[5]. Sanjekar, P. and J. Patil, *An Overview of Multimodal Biometrics.* Signal & Image Processing: An International Journal (SIPIJ) Vol, 2013. **4**: p. 57-64.

[6]. Hashim, H., S. Baker, and A. Nori, *Biometric identity Authentication System Using Hand Geometry Measurements.* Journal of Physics Conference Series, 2021. **1804**: p. 12144.

[7]. Okoh, E. and A.I. Awad. *Biometrics Applications in e-Health Security: A Preliminary Survey*. in *Health Information Science*. 2015. Cham: Springer International Publishing.

[8]. Manimekalai, S., *A study on biometric for single sign on health care security system.* Int J Comput Sci Mob Comput, 2014. **3**(6): p. 79-87.

[9]. Díaz-Palacios, J.R., V.J. Romo-Aledo, and A.H. Chinaei. *Biometric access control for e-health records in pre-hospital care*. in *Proceedings of the joint EDBT/ICDT 2013 workshops*. 2013.

[10]. Mason, J., et al., *An investigation of biometric authentication in the healthcare environment.* Array, 2020. **8**: p. 100042.

[11]. Heidari, H. and A. Chalechale, *Biometric authentication using a deep learning approach based on different level fusion of finger knuckle print and fingernail.* Expert Systems with Applications, 2022. **191**: p. 116278.

[12]. Alghamdi, M., P. Angelov, and L.P. Alvaro, *Person identification from fingernails and knuckles images using deep learning features and the bray-curtis similarity measure.* Neurocomputing, 2022. **513**: p. 83-93.

[13]. Kumar, S., S. Paul, and D.K. Shaw, *Design and Modeling of Real Time Multimodal Biometric Authentication System.* Journal of Computer Science, 2017.

[14]. Aparna, P. and P.V.V. Kishore, *Biometric-based efficient medical image watermarking in E-healthcare application.* IET Image Processing, 2019. **13**(3): p. 421-428.

[15]. Bhattasali, T., et al., *Bio-authentication for layered remote health monitor framework.* Journal of Medical Informatics and Technologies, 2014. **23**.

[16]. Srivastava, R. and D.K. Sharma. *Human Authentication Using Score Level Fusion of Face and Palm Print Biometrics*. in *VLSI, Microwave and Wireless Technologies*. 2023. Singapore: Springer Nature Singapore.

[17]. Al-Waisy, A., et al., *A Multimodal Biometric System for Personal Identification Based on Deep Learning Approaches*. 2017.

[18]. Shakil, K.A., et al., *BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud.* Journal of King Saud University - Computer and Information Sciences, 2020. **32**(1): p. 57-64.

[19]. Sarier, N.D., *Privacy Preserving Biometric Authentication on the blockchain for smart healthcare.* Pervasive and Mobile Computing, 2022. **86**: p. 101683.

[20]. Kurgan, L.A., K.J. Cios, and S. Dick, *Highly scalable and robust rule learner: performance evaluation and comparison.* IEEE Trans Syst Man Cybern B Cybern, 2006. **36**(1): p. 32-53.

[21]. Mamoudan, M.M., et al., *Food products pricing theory with application of machine learning and game theory approach.* International Journal of Production Research, 2022: p. 1-21.

[22]. Mousapour Mamoudan, M., et al., *Hybrid neural network-based metaheuristics for prediction of financial markets: a case study on global gold market.* Journal of Computational Design and Engineering, 2023. **10**(3): p. 1110-1125.

[23]. Rhayma, H., R. Ejbali, and H. Hamam, *Auto-authentication watermarking scheme based on CNN and perceptual hash function in the wavelet*

domain. Multimedia Tools and Applications, 2024: p. 1-23.

[24]. Agarwal, D., et al., *Automated Medical Diagnosis of Alzheimer´s Disease Using an Efficient Net Convolutional Neural Network.* Journal of Medical Systems, 2023. **47**(1): p. 57.

[25]. Mamoudan, M.M., et al., *Hybrid machine learning-metaheuristic model for sustainable agri-food production and supply chain planning under water scarcity*. Resources, Environment and Sustainability, 2023. **14**: p. 100133.

[26]. Pourkhodabakhsh, N., M.M. Mamoudan, and A. Bozorgi-Amiri, *Effective machine learning, Meta-heuristic algorithms and multi-criteria decision making to minimizing human resource turnover*. Applied Intelligence, 2023. **53**(12): p. 16309-16331.