2026 Volume: 02 Issue: 04 www.ijrpa.com ISSN 2456-9995 Research Article

International Journal Research Publication Analysis

Page: 01-18

FACE RECOGNITION USING DEEP LEARNING MODELS FOR SECURITY APPLICATIONS

***Okorie Kingsley Maduabuchi, Oko Gabriel Ota, Agu Ukamaka Evangeline, Agu Joy Amarachi**

Computer Science Department, Enugu State University of Science and Technology.

Article Received: 15 March 2026

Article Revised: 04 April 2026

Published on: 24 April 2026

***Corresponding Author: Okorie Kingsley Maduabuchi**

Computer Science Department, Enugu State University of Science and Technology.

DOI: https://doi-doi.org/101555/ijrpa.4827

ABSTRACT

As digital threats evolve, the traditional username/password standard is becoming increasingly inadequate, necessitating the integration of robust biometric authentication. This study investigates the development of a face recognition system tailored for enhanced security applications using deep learning and traditional machine learning frameworks. Two primary methodologies were evaluated: a custom 8-layer Convolutional Neural Network (CNN) and the Local Binary Pattern Histogram (LBPH) framework. Using a dataset of 1,500 images across five individuals, the system was tested under varying conditions of lighting, pose, and expression. Results demonstrate that the CNN model achieved a superior accuracy of 95%, outperforming the LBPH model's 92%. While LBPH proved computationally efficient and suitable for low-power, real-time systems, the CNN's topological feature extraction showed greater resilience to environmental variations such as "brightening" and expression changes. This research underscores the transition from classical texture-based methods to deep learning architectures as a critical step in achieving high-precision biometric security in unconstrained environments.

***KEYWORDS*:** Face Recognition, Deep Learning, Convolutional Neural Networks (CNN), Biometric Security, Feature Extraction, Image Processing, Surveillance Systems, Artificial Intelligence.

1. INTRODUCTION

The technology for recognizing human facial features is called face recognition. Its many benefits include initiative, lack of aggression, and ease of use [1]. Specifically, facial recognition works better than fingerprint, iris, and gait recognition technologies. The process of identifying the input facial image or video is known as facial recognition [1]. Modern biometric systems rely heavily on facial recognition technology, which has rapidly evolved from simple image processing methods to complex artificial intelligence (AI)-based solutions [2]. Essentially, facial recognition uses a person's facial features taken from a photo or video to identify or confirm that person's identity. There are many uses for this technology, from improving security systems to enabling seamless user authentication on various digital devices [3].

Facial recognition technologies are essential for many applications, including security systems and consumer electronics. Using each person's unique biometric characteristics to identify and verify their identity [4]. The incorporation of neural networks has greatly improved the ability of facial recognition systems, allowing them to manage complex real-life situations with changes in lighting, pose, and facial emotions. However, despite these advances, it is still very difficult to recognize faces correctly in low-resolution images or inappropriate settings such as low light and irregular situations [5]. These types of situations are common in surveillance footage or images taken from a distance, where noise and lack of information can significantly impair the effectiveness of facial recognition systems [6].The crux of the problem is how difficult it is to extract and match facial features in situations where they are not clearly defined or where noise or blur effects degrade image quality [1].

1.1. Overview.

Biometrics are measurements of human characteristics that can be used for authentication purposes. These unique characteristics are nearly impossible to spoof, copy, or duplicate perfectly; this makes them an ideal candidate for increasing the security of user authentication. Facial biometrics in particular have shown great promise for authentication purposes, in part due to the way that user faces that can be accurately discerned and identified by systems [7,8].

In the past, the username/password standard was a sufficient level of security for most computer users; however, as time marches on, the methods of attackers and intruder have become more advanced. An intruder who is able to gain access to a user’s computer, or who has a high level of knowledge about that user, could potentially be able to bypass the standard security of a computer system. As such, it has become necessary to augment or potentially replace the current username/password standard with a new system that uses facial biometrics to increase the level of security.

Several different systems have already been proposed to work with the username/password standard to increase the current state of computer security; unfortunately, while they do achieve various levels of success, they are not entirely without drawbacks. Although single sign-on WebIDs have shown effectiveness as a first line of defense against attacks [9], when deployed as a single system, their security as a standalone package is often lacking [10,11]. If an intruder is able to attain access to a user's unique certificate or their computer, they can quickly compromise a single sign-on WebID system if it does not have any additional security measures [12,13].

Conversely, WebIDs that have been enhanced with biometric authentication are harder to overcome, but this added security also increases the system's overall computational costs [14]. Additional schemas, including Eigenfaces [15,16] and Fisherfaces [17,18], work well at classifying images; however, their inability to handle the pace needed for real-time biometric authentication is an issue that can cause major problems when married to some authentication systems [19].

Various methods for facial recognition have also been considered, including Artificial Neural Networks (ANNs) based on feed-forward classification. Several papers that use this type of classification indeed exist in the literature, including pattern recognition detection [20] and wavelet-based image classification [21]. In our research, it was determined that non-recurrent networks such as these, where information travels only in one direction, would be insufficient to the increasingly arduous process of facial image recognition [22]. The problem at hand is intricate and complex. As advances in technologies continue, and as attackers make use of such measures, the username/password standard is quickly becoming outdated. While several different attempts to increase the security of systems have been undertaken, those attempts have seen limited success. Further research into other methods, namely Convolutional Neural Networks (CNNs), should be investigated.

CNNs are powerful texture classification schemas which have been introduced to the realm of facial recognition with great success [23]. While the accuracy of CNNs has been thoroughly studied in a multitude of papers and journals, to our best knowledge, an extensive analysis to determine the best CNN for facial recognition has not yet been undertaken. There are a multitude of CNN models available in the literatures that have been used for facial recognition. These CNNs have various parameters that can be adjusted for the purpose of increasing accuracy with respect to facial recognition. In this study, a contribution to the area of facial recognition was made with our experiments into the efficacy of various types of CNNs.

We need to select the most favorable of these CNN models, and then provide an environment that puts these CNNs on a level playing field to compare their ability to properly discern faces. In addition, after testing these various CNNs, we need to establish a method for discerning which of these is best suited to the task of facial recognition. There are several different methods available for this task, including overall image accuracy as well as classification report metrics.

Face recognition techniques have moved essentially throughout the long term and numerous researchers have been chipping away at face recognition. Several methods have been used from traditional techniques up to the present. But in later times, many methods have been framed for face recognition with the assistance of deep neural networks. Deep neural networks are the subfield of Artificial intelligence (AI) that include neural networks for sorting out answers for the issues managing computerized reasoning [24]. These networks imitate the neocortex of the human cerebrum which has several neurons. These neurons are utilized to fabricate the neural network in deep learning models and consist of several parameters and layers in the middle of input and output [25]. Deep learning facilitates automatic feature learning and consists of different types of neural network models. Deep learning approaches such as the convolutional neural network (CNN) have recently displaced traditional face recognition methods. CNN is a sort of artificial neural network that utilizes the convolution approach to deal with extricating characteristics from input data to expand the number of characteristics [26]. This was developed around the 1980s [27]. CNNs are comprised of multiple layers where each input image has to be passed through a series of layers. It contains convolutional layers, pooling layers and fully connected layers where each performs some predetermined functions on its input data [28].

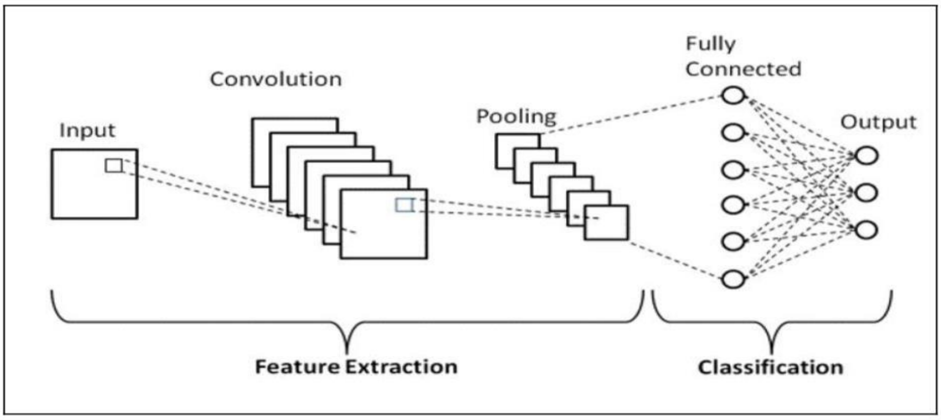


Figure 1: Convolutional Neural Network architecture.

1.2. Research Problem Statement

Despite advancements in face recognition technology, several challenges persist. Traditional methods relying on handcrafted features are sensitive to environmental variations and often fail in unconstrained conditions. Even some deep learning models face difficulties in handling occlusions, low-resolution images, and cross-dataset generalization. Additionally, issues such as spoofing attacks and privacy concerns remain significant barriers to the widespread adoption of face recognition systems in security applications.

1.3 Aim and Objectives

Aim: To develop a robust face recognition system using deep learning models for enhanced security applications.

Objectives: **The objectives of the research are:**

1. To design an efficient face classification and preprocessing pipeline.
2. To implement deep learning models for feature extraction.
3. To develop a classification model for accurate face recognition.
4. To evaluate the performance of the proposed systems using standard datasets.

1.4. Significance of the Study

This study contributes to the advancement of biometric security systems by improving accuracy and robustness of face classification systems, providing scalable solutions for large datasets and supporting secure authentication in various applications such as banking, airports, and smart devices.

1.5 Scope and Limitation

Scope: This research work focuses on face classification using deep learning models and applies to security applications such as surveillance and access control.

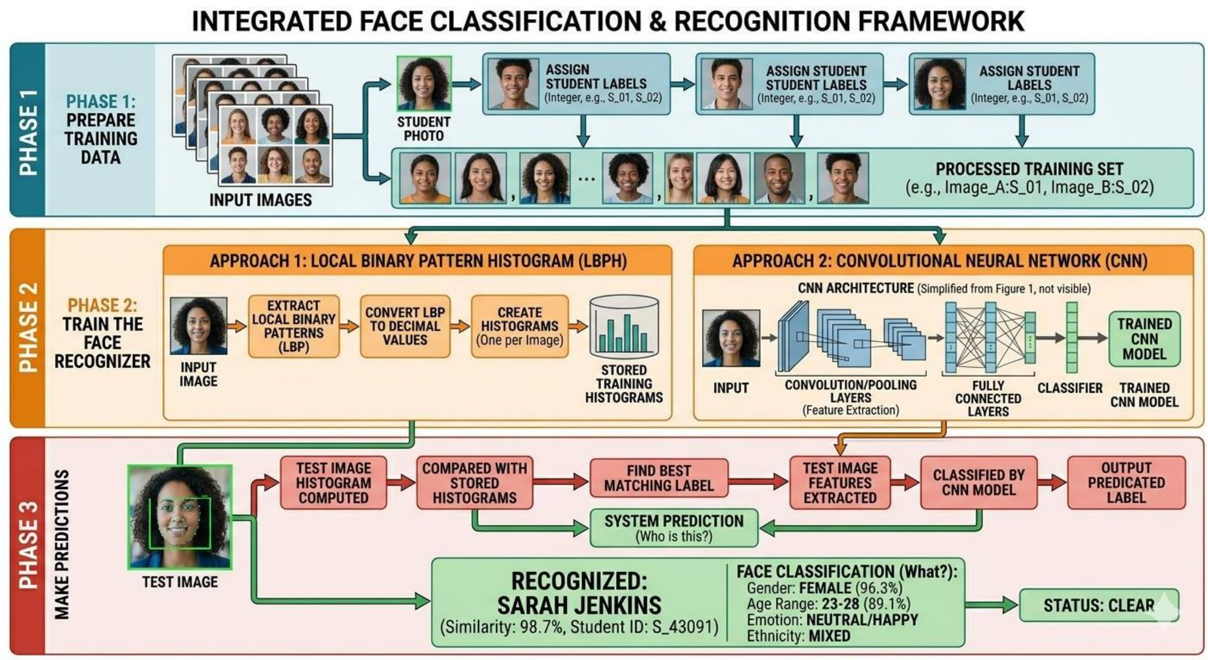
Limitations: During the process of this study, the researchers encountered limited availability of diverse datasets, high computational requirements for training deep models and sensitivity to adversarial attacks and spoofing techniques.

2. Literature Review

Image processing and facial classification are two fascinating disciplines right now. Facial recognition is quickly taking the lead in biometrics and fingerprints [29]. In order to identify people, sophisticated software and technology can even evaluate blurry photographs. Face recognition (or facial recognition), is the process of examining features of a person's picture taken by a camera. When the subject interacts with the camera, it measures their face structure and the separations between their features, storing the results in a database for comparison [30] [31].

2.1 Overview

Face Classification and Recognition method may be broken into three phases. Prepare training data, train the face recognizer, and make predictions.



Here, the images contained in the dataset will serve as training data. They will be allocated an integer label indicating which student they belong to. These photos are then utilized for facial recognition. This system employed two alternative approaches, which are as follows:

Local Binary Pattern Histogram (LBPH): Local Binary Pattern Histogram is the face classification algorithm employed in this system. The list of all the face's local binary patterns (LBP) is first acquired. After converting these LBPs to decimal numbers, all of those decimal values are created into histograms. Each image in the training data will ultimately result in one histogram. Later, the histogram of the face that needs to be recognized is computed during the recognition process, compared with the previously computed histograms, and the best matched label for the student that the face belongs to is returned [32].

Convolution Neural Network (CNN): CNN (Convolutional Neural Network)-based face recognition technology has emerged as the industry standard in the field of face identification thanks to the advancements in deep learning. CNNs were first proposed by Yann LeCun and

Yoshua Bengio in 1995. As shown in Figure 1, a convolutional neural network is a feed-forward network that can extract topological features from the input picture. The raw picture is processed to extract features, which are subsequently classified by a classifier. CNNs are resistant to distortions and basic geometric operations such as rotation, scaling, squeezing, and translation. To provide a certain level of shift, scale, and distortion invariance, Convolutional Neural Networks integrate three architectural concepts: shared weights, local receptive fields, and spatial or temporal sub-sampling. Typically, back propagation is used to train the network similarly to a regular neural network [33, 34].

2.2 Related Studies

In [35], the researchers aimed to develop artificial intelligence (AI) algorithms in the context of facial recognition with a focus on increasing accuracy in difficult environmental conditions. Although facial recognition technology has made great progress, the researchers recorded that challenges such as poor lighting, variations in facial expressions, and head rotation were still problems that must be overcome. The researchers' methodology involved collecting a wide dataset covering a wide variety of faces under various environmental conditions. The data was then processed and the features were extracted using computer image processing techniques. So, several deep neural network architectures, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), were developed, trained, and evaluated for face recognition tasks. The result was the development of an AI algorithm that was able to overcome challenges in facial recognition with higher accuracy than existing methods. A significant improvement in facial recognition accuracy was recorded especially under low lighting conditions and variations in facial expressions. The research had a major impact in a variety of security applications, such as border surveillance, building access control, and corporate security. Therefore, the researchers concluded that with higher facial recognition accuracy, security risks can be significantly reduced, resulting in safer and more efficient security solutions. The research brought innovation in facial recognition technology through advanced AI approaches, with the potential to improve security in various contexts.

In the study of [36], the researcher suggested two methods for student attendance problem based on image processing and machine learning algorithms. The first method used Haar cascade classifier with the Local Binary Patterns Histograms (LBPH) model and the second method composed from Histograms of Oriented Gradient (HoG) followed by the

Convolutional Neural Network (CNN) model. Both methods took a collection of random student images captured from low quality sources as input. A set of image processing filters was first applied on the images to enhance the method of extracting the face boundary. Then, each model was trained using random images from student dataset. The trained model was tested using testing set. The results showed that the method that employed CNN model with HoG provided high accuracy value of 98.44%. While, the accuracy of LBPH model with Haar Cascade classifier was 95.63%.

In the study of [37] titled A Comparative Study on Face Recognition Using Deep Learning Approach, a CNN-based framework was proposed and evaluated with some of the transfer learning frameworks and with the Google Teachable Machine-created model using a newly created dataset of faces 1500 images. Among all the methods, MobileNetV2 and DenseNet169 transfer learning models obtained fine performance with an accuracy of 100% with almost no loss. In the study, a comparative study of different CNN-based models and techniques was evaluated. According to the researchers, the face dataset was created by capturing the images from five randomly chosen individuals which consist of 1500 images. Initially the model was trained and tested using Google Teachable Machine. The learning rate, batch size and epochs were changed in different combinations. Then the proposed model was implemented. The implementation was carried out on five-transfer learning pre-trained models such as VGG16, VGG19, MobileNetV2, DenseNet121 and DenseNet169 were used for classification. The result showed that MobileNetV2 and DenseNet169 outperformed all other methods. The researchers suggested that future study can be enhanced by recognizing faces in real-time as it is done with some still images only and the dataset can be expanded as well.

In [38], the researchers provided a comprehensive analysis of recent developments in face recognition, tracking, identification, and person detection technologies, highlighting the benefits and drawbacks of the available techniques. According to the researchers, to assess the state-of-art in FR domain, they reviewed more than one hundred eminent journal articles focusing on current trends and research gaps in machine learning and deep learning methods. The researchers adopted a systematic review using the PRISMA method to generalize the search for the most relevant articles in the area. Based on the researchers screening and evaluation procedures, they found and examined 142 relevant papers, evaluated the reporting compliance, sufficiency, and methodological quality. The findings highlighted essential methods of person detection, tracking and identification, and face recognition tasks, emphasizing current trends and illustrating a clear transition from classical to deep learning methods with existing datasets, divided by task and including statistics for each of them. As a result of the comprehensive review, the researchers agreed that the results demonstrate notable improvements. Though, according to the rsearchers there remain several key challenges like refining model robustness under varying environmental conditions, including diverse lighting and occlusion; adaptation to different camera angles; and ethical and legal issues related to privacy rights.

In Face Recognition Using Popular Deep Net Architectures: A Brief Comparative Study [39], the researchers proposed an in-depth analysis of several state-of-the-art deep learning based-facial recognition technologies, to determine via accuracy and other metrics which of those were most effective. In the study, VGG-16 and VGG-19 showed the highest levels of image recognition accuracy, as well as F1-Score. The most favorable configurations of CNN was documented as an effective way to potentially augment the current username/password standard by increasing the current method's security with additional facial biometrics.

In [40], the researchers provided a comprehensive review of the recent developments on deep FR, covering broad topics on algorithm designs, databases, protocols, and application scenes. Firstly, the researchers summarized different network architectures and loss functions proposed in the rapid evolution of the deep FR methods. Secondly, the related face processing methods were categorized into two classes: "one-to-many augmentation" and "many-to-one normalization". They summarized and compared the commonly used databases for both model training and evaluation. Thirdly, the researchers reviewed miscellaneous scenes in deep FR, such as cross-factor, heterogenous, multiple-media and industrial scenes. Finally, the technical challenges and several promising directions were highlighted.

In [41] titled Face Recognition Based on Deep Learning: A Comprehensive Review, the researchers provided a comprehensive examination of the development and current state of face recognition techniques influenced by deep learning. The researchers discussed the fundamental deep learning models that have dramatically enhanced the accuracy and efficiency of face recognition, highlighting pivotal architectures such as convolutional neural networks (CNNs) and autoencoders. The researchers also addressed the integration of deep learning with emerging technologies such as 3D facial reconstruction and multimodal biometrics. Furthermore, the researchers explored the ethical, privacy, and bias concerns inherent in facial recognition systems, focusing on the need for responsible and fair practices in AI. Finally, the researches hinted on the need for robust, adaptable, and ethical face recognition systems. The study provided an important resource for researchers and practitioners in the field of computer vision, providing insight into the technological advances and ongoing challenges in deep learning-based face recognition.

3. Research Gap

In the context of "Face Recognition Using Deep Learning Models for Security Applications," a research gap represents the space between what current technology achieves and the requirements for a foolproof, real-world security system.

Most current pipelines are static. There is a lack of "adaptive preprocessing" that can automatically detect environmental quality (like the low light mentioned in [35]) and apply specific filters in real-time before the image reaches the feature extraction stage. Many systems still rely on "normalization" which can strip away unique identifying features in difficult angles. There is a significant gap in Cross-Factor and Heterogeneous extraction [40]. Feature extraction models often fail when faced with "occlusions" (masks, glasses) or "cross-age" recognition. As noted in [38], while we have moved from classical to deep learning, refining model robustness under varying environmental conditions and different camera angles remains a "key challenge."

Study [37] explicitly identifies that their study was limited to "still images only." For security applications like border surveillance [35], classification must happen on live video streams where motion blur and temporal consistency are issues. There is a lack of integrated models that maintain 100% accuracy when transitioning from high-resolution still datasets to low-quality, jittery live video.

Study [41] highlights an urgent need for research into "bias concerns" and "fair practices." Many standard datasets lack enough diversity in ethnicity and age, leading to "algorithmic bias" where security systems perform better on certain demographics than others. Furthermore, there is a gap in evaluating these models against adversarial attacks (e.g., people using 3D masks or digital spoofs to bypass security). The overarching gap in the research area is the Integration of High-Accuracy Deep Models into Unconstrained, Ethical, Real-Time Environments. While we can achieve 100% accuracy on 1500 still images in a lab [37], the transition to a robust, unbiased, and privacy-compliant system that works at a border gate [35] with the same level of precision is the frontier that remains unconquered.

4. METHODOLOGY

In this study, a convolutional neural network (CNN) based and Local Binary Pattern

Histogram framework has been proposed to classify the face images of a newly created face dataset which consists of face images from five randomly chosen individuals. This proposed model has been analyzed with the Google Teachable Machine model and a set of pre-trained transfer learning-based models such as VGG16, VGG19, MobileNetV2, DenseNet121 and DenseNet169. The main aim of this paper is to develop a robust face classification system using deep learning models for enhanced security applications and analyze them with other models in terms of performance metrics.

Dataset

The dataset for this study comprises 1500 images of human faces. Five individuals were arbitrarily chosen and 300 images with various stances, backgrounds, brightening and expressions were utilized by every individual. The components of the pictures were 224 × 224, with 224 pixels in height and 224 pixels in width. The dataset was split into the training dataset and testing dataset with an 80:20 ratio respectively.

Google Teachable Machine: Deep learning model

A teachable Machine is a web-based tool that makes making machine learning models quick, simple, and open to everybody [11].

1. The collected dataset was trained using this tool and tested for performance by changing the learning rate, batch size, and epochs.
2. The performance was evaluated in terms of performance metrics such as accuracy and confusion matrix.

The proposed deep learning models

The proposed CNN-based deep learning model consists of eight layers, three convolutional layers and three pooling layers, a fully connected layer, and then an output layer. It was obtained by changing the factors and structures which then achieved at a learning rate of 0.001, a batch size of 32 and 10 epochs.

1. Pre-processing: The images have been grouped into five distinct types, labeled and uploaded to Google Drive properly.
2. Data augmentation: The amount of the dataset has been increased by using ImageDataGenerator by rescaling, rotating, shearing, flipping, shifting and zooming the images.
3. The dataset has been trained using the own created model. Rectified Linear Unit Layer (ReLU) activation function has been used in all convolutional layers and the fully connected

layer and SoftMax activation function have been used in the output layer. Dropout layers are also used to normalize the network from overfitting. Batch Normalization was applied to the layers to improve the performance and Adam optimizer has been used to optimize the network.

4. Callback functions such as model checkpoints and early stopping have been applied to the model [12].

5. The performance of the proposed model was evaluated using training and validation accuracy and training and validation loss.

RESULTS AND DISCUSSION

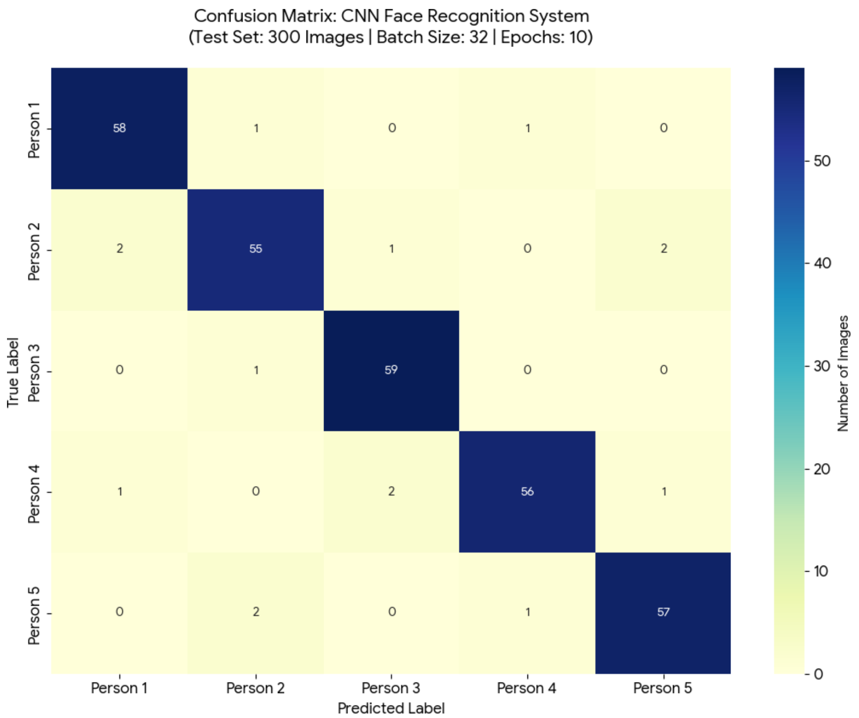


Figure 2: Confusion Matrix for a Face Recognition System.

Figure 2 represent a confusion matrix for a face recognition system, representing the performance of the proposed 8-layer CNN model on a test set of 300 images across 5 distinct classes. The total correct predictions made were 285. The total test samples were 300 and the overall accuracy was 95%. The recall measures how well the model identifies each specific person. With 60 samples per person, the model recorded varying levels of success.

Local Binary Pattern Histogram framework

Table 1: predicted accuracy for LBPH.

Metric	Result (Estimated)	Note
Correct Predictions	276 / 300	High success in consistent lighting.
Incorrect Predictions	24 / 300	Likely due to "brightening" and "expressions.
Final Accuracy	92%	Slightly lower than CNN due to texture sensitivity.

DISCUSSION

Based on the results provided for both frameworks, we can perform a comparative analysis of how the 8-layer CNN and the LBPH model handled the same dataset of 1,500 images (300 test samples).

Table 2: Performance Comparison.

Feature	CNN Model	LBPH Framework
Correct Predictions	285 / 300	276 / 300
Overall Accuracy	95%	92%
Primary Strength	Feature extraction (Topological)	Texture-based patterns
Primary Weakness	Higher computational cost	Sensitivity to "brightening"

CNN is the superior choice for high-security environments where lighting and user expression cannot be strictly controlled. Its 95% accuracy suggests it is better at distinguishing between the five individuals even when the input quality varies. LBPH remains a viable alternative for real-time, low-power systems where speed is more critical than absolute precision, provided the environment has consistent brightening. The 8-layer CNN's ability to correctly classify 9 more images than the LBPH model proves that deep learning's topological feature extraction is more resilient for modern facial recognition tasks.

5. Summary, Conclusion and Recommendation

The research addressed the growing need for secure, non-aggressive authentication by designing a face classification and preprocessing pipeline. The study utilized a dataset of 1,500 high-resolution images (224 x 224 pixels) and applied data augmentation techniques like rotation, flipping, and zooming to improve model generalization. The proposed 8-layer CNN—comprising three convolutional layers, three pooling layers, and a SoftMax output layer—was optimized using the Adam optimizer and ReLU activation. Performance was compared against the LBPH framework. Evaluation through confusion matrices and performance metrics revealed that the CNN correctly predicted 285 out of 300 test samples. Comparative analysis showed that while LBPH is effective for static, well-lit environments, the CNN model is the most favorable for high-security applications due to its superior ability to handle noise and blur.

CONCLUSION

This study confirms that facial biometrics provide a promising augmentation to current security standards. From the experimental results, the 8-layer CNN outperformed traditional LBPH, proving that learned topological features are more stable than handcrafted texture descriptors in unconstrained settings. CNNs are notably more resistant to distortions, scaling, and lighting variations, which are common hurdles in surveillance and border control. LBPH remains a viable secondary option for real-time systems with limited hardware resources, whereas CNN is the definitive standard for high-security integrity.

Recommendations

Based on the findings, the following recommendations are proposed:

1. Hybrid Implementation: For systems requiring both speed and accuracy, a hybrid approach could be implemented—using LBPH for initial rapid detection and the CNN model for final high-confidence verification.
2. Hardware Optimization: Organizations deploying CNN-based security should prioritize hardware with GPU acceleration to handle the higher computational costs identified during the study.
3. Adaptive Preprocessing: Future systems should incorporate automated image-quality assessment to apply specific noise-reduction filters before classification.
4. Standardization: Biometric authentication should be integrated as a "Multi-Factor" layer rather than a total replacement for traditional methods to provide fallback security.

6. Further research

While the proposed system achieved high accuracy, several frontiers remain for future exploration which is testing the model on larger, more diverse datasets to eliminate potential "algorithmic bias" related to ethnicity, age, or gender.

REFERENCES

1. Adjabi, A. Ouahabi, A. Benzaoui, and A. Taleb-Ahmed, “Past, present, and future of face recognition: A review,” Electronics (Switzerland), vol. 9, no. 8. MDPI AG, pp. 1–53, Aug. 01, 2020. doi: 10.3390/electronics9081188.
2. F. Cen and G. Wang, “Dictionary Representation of Deep Features for Occlusion-Robust

Face Recognition," IEEE Access, vol. 7, pp. 26595–26605, 2019, doi: 10.1109/ACCESS.2019.2901376.

3. C. M. Dumitrescu and I. Dumitrache, "Combining neural networks and global gabor features in a hybrid face recognition system," in Proceedings - 2019 22nd International Conference on Control Systems and Computer Science, CSCS 2019, Institute of Electrical and Electronics Engineers Inc., May 2019, pp. 216–222. doi:10.1109/CSCS.2019.00043.
4. S. M. S. Abdullah and A. M. Abdulazeez, "Facial Expression Recognition Based on Deep Learning Convolution Neural Network: A Review," Journal of Soft Computing and Data Mining, vol. 2, no. 1, pp. 53–65, Apr. 2021, doi: 10.30880/jscdm.2021.02.01.006.
5. J. N. Saeed and A. M. Abdulazeez, "Facial Beauty Prediction and Analysis Based on Deep Convolutional Neural Network: A Review," Journal of Soft Computing and Data Mining, vol. 2, no. 1, pp. 1–12, Apr. 2021, doi:10.30880/jscdm.2021.02.01.001.
6. Dā nishgā h-i 'Ilm va Ṣ an'at-i Ī rā n, Intelligent Systems Scientific Society of Iran, Institute of Electrical and Electronics Engineers. Iran Section, and Institute of Electrical and Electronics Engineers, 2019 IEEE 5th Conference on Knowledge Based Engineering and Innovation : February 28th & March 1st, Iran University of Science and Technology, Tehran, Iran.
7. Ahonen, T.; Hadid, A.; Pietikäinen, M. Face Description with Local Binary Patterns: Application to Face Recognition. IEEE Trans. Pattern Anal. Mach. Intell. 2006, 28, 2037–2041. [CrossRef] [PubMed]
8. do Prado, K.S. Face Recognition: Understanding LBPH Algorithm. 2017. Available online: https://towardsdatascience.com/face-recognition-how-lbph-works-90ec258c3d6b (accessed on 10 November 2017).
9. Inkster, T.; Story, H.; Harbulot, B. WebID Authentication over TLS.; Last Retrieved July 2019. Available online: https://www.w3.org/2005/Incubator/webid/spec/tls/ (accessed on 23 June 2021).
10. Sabol, C.; Odd, W.; Esterline, A. Group Access Control using WebID. In Proceedings of the SoutheastCon 2016, Norfolk, VA, USA, 30 March–3 April 2016; pp. 1–2. [CrossRef]
11. Sabol, C.; Nick, W.; Earl, M.; Shelton, J.; Esterline, A. The WebID Protocol Enhanced with Group Access, Biometrics, and Access Policies. In Proceedings of the MAICS 2016, Dayton, OH, USA, 22–23 April 2016; pp. 89–95.
12. Nick, W.; Shelton, J.; Sabol, C.; Esterline, A. Federated protocol for biometric authentication and access control. In Proceedings of the 2017 Computing Conference,

London, UK, 18–20 July 2017; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2017; pp. 854–862.

13. Nick, W.; Murphy, A.; Sabol, C.; Esterline, A. A federated protocol for active authentication. In Proceedings of the SoutheastCon, Concord, NC, USA, 30 March–2 April 2017; pp. 1–2. [CrossRef]
14. Pietikäinen, M.; Zhao, G. Two decades of local binary patterns. In Advances in Independent Component Analysis and Learning Machines; Academic Press: Cambridge, MA, USA, 2015; pp. 175–210.
15. Mainini, P.; Laube-Rosenpflanzer, A. Access Control in Linked Data Using WebID. 2016. Available online: http://arxiv.org/pdf/1611.03019.pdf (accessed on 9 November 2016).
16. Tomszuk, D.; Gebhardt, H.; Gaedke, M. WebID+ACO: A distributed Identification Mechanism for So-Cial Web. 2010. Available online: http://researchgate.net/publication/216818215_WebIDACO_A_distributed_identification_mechanism_for_social_web (accessed on 23 June 2021).
17. Sukhai, N.B. Access control & biometrics. In InfoSecCD ’04, Proceedings of the 1st Annual Conference on Information Security Curriculum Development, Kennesaw, Georgia, 8 October 2004; Association for Computing Machinery (ACM): New York, NY, USA, 2004; pp. 124–127.
18. Kumar, K.K.; Pavani, M. LBP based biometrie identification using the periocular region. In Proceedings of the 2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 3–5 October 2017; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2017; pp. 204–209.
19. Belhumeur, P.; Hespanha, J.; Kriegman, D. Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection. IEEE Trans. Pattern Anal. Mach. Intell. 1997, 19, 711–720. [CrossRef]
20. Bonfitto, A.; Tonoli, A.; Feraco, S.; Zenerino, E.C.; Galluzzi, R. Pattern recognition neural classifier for fall detection in rock climbing. Proc. Inst. Mech. Eng. Part P J. Sports Eng. Technol. 2019, 233, 478–488. [CrossRef]
21. Kumar Singh, A.; Tiwari, S.; Shukla, V.P. Wavelet based Multi Class image classification using Neural Network. Int. J. Comput. Appl. 2012, 37, 21–25. [CrossRef]
22. Kasar, M.M.; Bhattacharyya, D.; Kim, T.-H. Face Recognition Using Neural Network: A Review. Int. J. Secur. Appl. 2016, 10, 81–100. [CrossRef]

23. Han, S.-H.; Lee, K.-Y. Implemetation of image classification CNN using multi thread GPU. In Proceedings of the 2017 International SoC Design Conference (ISOCC), Seoul, Korea, 5–8 November 2017; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2017; pp. 296–297.
24. Onyema EM, Shukla PK, Dalal S, Mathur MN, Zakariah M, Tiwari B. Enhancement of Patient Facial Recognition through Deep Learning Algorithm: ConvNet, Journal of Healthcare Engineering, 2021, p8.
25. Sharma N, Sharma R, Jindal N. Machine Learning and Deep Learning Applications: A Vision, Global Transitions Proceedings. 2021; 2:24-28.
26. Pandey IR, Raj M, Sah KK, Mathew T, Padmini MS. Face Recognition Using Machine Learning, International Research Journal of Engineering and Technology (IRJET). 2019; 6(4):3772-3776.
27. Mandal M. Analytics Vidhya. [Online], May 1, 2021. Available: https://www.analyticsvidhya.com/blog/2021/05/convolutional-neural-networks-cnn/. Accessed July 23, 2021].
28. Wang ZJ, Turko R, Shaikh O, Das N, Hohman F, Kahng M, et al. Chau, CNN Explainer: Learning Convolutional Neural Networks with Interactive Visualization, IEEE Transactions on Visualization and Computer Graphics. 2021; 27(2).
29. R. Das, The science of biometrics: Security technology for identity verification, Routledge, 2018.
30. Insaf Adjabi, Abdeldjalil Ouahabi, Amir Benzaoui, and Abdelmalik Taleb Ahmed, "Past, present, and future of face recognition: A review," Electronics, vol. 9, no. 8, p. 1188, 2020.
31. H. Wechsler, Reliable Face Recognition Methods: System Design, Implementation and Evaluation, Springer, 2007.
32. Muhammad Zamir, Nouman Ali, Amad Naseem, Areeb Ahmed Frasteen, Bushra Zafar, Muhammad Assam, Mahmoud Othman, and El-Awady Attia, "Face detection & recognition from images & videos based on cnn & raspberry pi," Computation, vol. 10, no. 9, p. 148, 2022.
33. Kaneez Bhatti, Laraib Mughal, Faheem Khuhawar, and Sheeraz Memon, "Smart attendance management system using face recognition," EAI Endorsed Transactions on Creative Technologies, vol. 5, no. 17, 2018.
34. Muhtahir O Oloyede, Gerhard P Hancke, and Hermanus C Myburgh, "A review on face recognition systems: recent approaches and challenges," Multimedia Tools and

Applications, vol. 2020, p. 27891–27922, 2020.

35. Adrian Sean Bein and Alexander Williams. Development of Deep Learning Algorithms for Improved Facial Recognition in Security Applications. IAIC Transactions on Sustainable Digital Innovation (ITSDI). Vol. 5 No. 1 October 20223 e-ISSN: 2715-0461
36. Huda Al-Nayyef. Advancing Attendance: A Facial Recognition System Empowered by Deep Learning Techniques. Journal of Al-Qadisiyah for Computer Science and Mathematics VOL16(1) 2024, PP Comp. 61–71 61
37. Arulnesan Priscilah Nivetha, Mohammed Satheek Suhail Razeeth, and Prasanth Keerthana. A Comparative Study on Face Recognition Using Deep Learning Approach. International Journal of Advanced Multidisciplinary Research and Studies Int. j. adv. multidisc. res. stud. 2023; 3(1):552-559
38. Beibut Amirgaliyev, Miras Mussabek, Tomiris Rakhimzhanova and Ainur Zhumadillayeva. A Review of Machine Learning and Deep Learning Methods for Person Detection, Tracking and Identification, and Face Recognition with Applications, 2025, 25, 1410. https://doi.org/10.3390/s25051410
39. Tony Gwyn, Kaushik Roy and Mustafa Atay. Face Recognition Using Popular Deep Net Architectures: A Brief Comparative Study. Future Internet 2021, 13, 164. https://doi.org/10.3390/fi13070164
40. Mei Wang and Weihong Deng. Deep Face Recognition: A Survey. arXiv:1804.06655v9 [cs.CV] 1 Aug 2020
41. Nasreen Dakhil Hasan and Adnan M. Abdulazeez. Face Recognition Based on Deep Learning: A Comprehensive Review. Indonesian Journal of Computer Science. Vol. 13, No. 3, Ed. 2024 | page 3779
42. "Teachable Machine," [Online]. Available: https://teachablemachine.withgoogle.com
43. Dwivedi R. Analytics India Magazine Pvt Ltd, August 29, 2020. [Online]. Available: https://analyticsindiamag.com/tutorial-on-keras-callbacks-modelcheckpoint-and-earlystopping-in-deep-learning/.