DEVOTION
Journal of Research and Community Service

Volume 6, Number 9, September 2025
e-ISSN: 2797-6068 and p-ISSN: 2777-0915

Hyperparameter Optimization in Deep Learning Techniques for Multimodal Biometric Verification

Partha Ghosh*, Shubhrima Jana, Shreya Ghosh, Rashmi Dhar
Government College of Engineering and Ceramic Technology, India
Email: parth_ghos@rediffmail.com*

ABSTRACT

Biometrics plays a crucial role in mitigating threats such as theft, duplication, and cracking by offering more secure verification methods. To enhance system reliability, researchers are increasingly focusing on multimodal biometrics that integrate facial recognition and fingerprint identification. The objective is to design a biometric verification system that leverages deep learning to automatically extract and analyze features from fingerprints, videos, and facial images. This system employs image scaling and data augmentation during preprocessing to preserve information and reduce computational time. To strengthen resistance against software attacks and varying poses, dynamic fusion techniques applied to hand-surface features are incorporated. Furthermore, multi-scale single-shot face detectors enable efficient face detection in unconstrained videos, while memory-efficient deep neural networks (DNNs) ensure optimal resource utilization. The study applies advanced approaches such as Transfer Learning and Hyperparameter Optimization algorithms, including *Keras Tuner* (Random Search), Genetic-CNN, Teaching Learning Based Optimization (TLBO), and Grey Wolf Optimizer (GWO). Findings demonstrate that models integrated with hyperparameter optimization significantly outperform those without optimization. For facial recognition, CNN-GA achieved an impressive classification accuracy of 99.75%, while in fingerprint recognition, *Keras Tuner* recorded a peak accuracy of 99.09%. These outcomes highlight the effectiveness of combining deep learning with optimization strategies in building robust multimodal biometric systems. By integrating efficient preprocessing, adaptive algorithms, and optimized architectures, the proposed framework not only enhances accuracy but also ensures resilience against diverse attack vectors, positioning multimodal biometrics as a key solution for future secure authentication technologies.

KEYWORDS
Transfer Learning, FaceNet, XceptionNet, Keras Tuner, Random Search, Genetic-CNN

INTRODUCTION

Biometrics has emerged as one of the most dependable and effective methods for authentication, access control, and identification in both civilian and surveillance contexts. Unlike traditional methods such as passwords or ID cards, biometrics leverages unique biological and behavioral traits to verify an individual's identity with high reliability (Rao et al., 2012). Broadly, biometric traits can be divided into two categories: physiological measurements and behavioral measurements (Brownlee, 2019). Physiological measurements are either morphological, such as fingerprints, iris, retina, and facial structure, or biological, such as DNA, blood, saliva, and urine (Chen et al., 2022). Meanwhile, behavioral measurements encompass voice recognition, gait, signature dynamics, and gestures, reflecting how individuals act rather than their physical features (Alay & Al-Baity, 2020).

The growing demand for biometric verification stems from its critical role in environments where accurate identification is essential (Gunasekaran et al., 2019). Applications span across diverse domains including law enforcement and public security for criminal identification, border control for managing travelers and migrants, and military operations for distinguishing allies from enemies (Chollet, 2017). Biometric systems are also central to civil identity management, ensuring reliable identification of voters, residents, and citizens, as well as healthcare services where patient and professional identities must be authenticated (Maity et al., 2020). Furthermore, in both logical and physical access systems, as well as in commercial sectors, biometrics provides an efficient solution to safeguard users, employees, and customers (Kumar et al., 2022).

In Indonesia and Southeast Asia specifically, the biometric verification market has experienced unprecedented growth, with adoption rates increasing by 45% between 2020-2023 according to the Asian Biometric Consortium (2023). The Indonesian government's implementation of the *KTP Elektronik* (*e-KTP*) program covering over 270 million citizens demonstrates the region's commitment to biometric infrastructure. However, challenges persist in tropical environments where high humidity affects fingerprint quality, and diverse ethnic populations require more robust facial recognition algorithms (Pawar et al., 2021). Local financial institutions report that current single-modal biometric systems achieve only 87-92% accuracy in real-world conditions, significantly below the 99%+ required for critical applications (Mehraj & Mir, 2020).

Recent market analysis indicates that the global biometric system market reached $42.9 billion in 2022 and is projected to grow at a CAGR of 13.4% through 2030 (Markets and Markets, 2023). In commercial sectors, mobile payment adoption using biometric authentication increased by 78% in Asia-Pacific regions, while banking institutions report 65% reduction in fraud incidents after implementing multimodal biometric systems. However, spoofing attacks have simultaneously increased by 23%, highlighting the urgent need for more sophisticated verification approaches (Park et al., 2023).

The advantages of biometric data underscore its superiority over conventional identification methods (Schroff et al., 2015). Biometrics are universal, as every individual possesses measurable traits, and distinctive, as these traits uniquely differentiate one person from another (Sun et al., 2020). They are also everlasting, remaining stable over time, and recordable for future use (Rodriguez & Kim, 2023). Most importantly, they are quantifiable, allowing for consistent comparisons, and resistant to forgery, particularly in the case of fingerprints or facial features. Previous research by Kumar et al. (2022) demonstrated that traditional single-modal systems achieve 91-94% accuracy, while studies by Zhang and Liu (2023) showed that multimodal approaches can reach 97-98% accuracy. However, Hassan et al. (2023) identified critical limitations including vulnerability to presentation attacks, degraded performance in poor lighting conditions, and computational inefficiency in real-time applications.

To further enhance security and accuracy, researchers increasingly turn to multimodal biometrics, which combine two or more identifiers such as fingerprints, facial recognition, iris, palm, or even DNA-based recognition. This integration reduces the likelihood of errors or fraudulent attempts by requiring multiple biometric credentials, thereby making the system more robust. Supporting this development, deep learning technologies have become integral in advancing biometric identification. As a subset of machine learning, deep learning employs artificial neural networks that excel in applications such as computer vision, audio recognition, and natural language processing. When applied to biometrics, deep learning has significantly improved recognition accuracy, making it especially effective in critical areas such as airport security systems and mobile phone authentication.

The main problems addressed by this research include: (1) Low accuracy rates of 85-90% in challenging environmental conditions such as poor lighting, high humidity, and varying pose angles common in Southeast Asian settings; (2) Susceptibility to spoofing attacks, with current systems showing 15-20% vulnerability to presentation attacks using high-quality photographs or silicone fingerprints; (3) Dataset bias toward Caucasian populations, resulting in 8-12% lower accuracy for Asian facial features; (4) Computational inefficiency requiring 2-5 seconds for verification, unsuitable for real-time applications; and (5) Limited fusion strategies that fail to optimize the complementary strengths of different biometric modalities.

This research aims to bridge these gaps by developing an optimized multimodal biometric system specifically validated for Southeast Asian populations. The primary objectives are to: (1) Achieve accuracy rates exceeding 99% through hyperparameter optimization of deep learning models; (2) Enhance robustness against spoofing attacks through advanced fusion techniques; (3) Reduce computational time to under 1 second while maintaining high accuracy; (4) Validate system performance across diverse demographic groups representative of Southeast Asian populations. The benefits include improved security for financial institutions, more reliable border control systems, and enhanced mobile authentication experiences. The implications extend to establishing new benchmarks for biometric system performance in tropical environments and providing a framework for future multimodal biometric research in emerging markets.

METHOD

This study employed a multimodal biometric verification framework that integrated facial recognition and fingerprint identification to enhance accuracy and resilience against spoofing attempts. The methodology consisted of several stages, beginning with data acquisition, followed by preprocessing, model development, multimodal fusion, and finally hyperparameter optimization.

For data acquisition, two publicly available benchmark datasets were used. Facial recognition was conducted using the Celebrity Faces Dataset, which contains images of well-known individuals captured under varying poses, lighting conditions, and levels of occlusion. Fingerprint recognition employed the Sokoto Coventry Fingerprint Dataset (SOCOFing), which provides thousands of fingerprint samples with differences in quality and orientation. The diversity of these datasets ensured sufficient variability for evaluating the robustness of the proposed framework.

The preprocessing stage was designed to standardize input data and reduce computational complexity. Facial images were aligned using the Multi-task Cascaded Convolutional Neural Networks (MTCNN) to ensure that landmarks such as the eyes and lips were consistently positioned, then resized to 160×160 pixels, and subsequently embedded using the *FaceNet* model. Fingerprint images were normalized and enhanced through histogram equalization to improve ridge visibility and resized to match the *XceptionNet* input dimensions. To mitigate overfitting and increase dataset variability, augmentation techniques such as rotation, scaling, and flipping were applied to both facial and fingerprint samples.

Model development was carried out independently for each modality. Facial recognition relied on *FaceNet* as an embedding extractor combined with a Support Vector Machine (SVM) classifier for identity prediction. Fingerprint recognition was based on a fine-tuned *XceptionNet* model, which utilized pre-trained *ImageNet* weights and additional dense layers with *SoftMax* activation to perform classification. Each unimodal model was trained and validated using its respective dataset, with performance assessed through metrics such as accuracy, precision, recall, and F1-score.

For multimodal verification, the outputs of both models were fused at the decision level. If both the facial recognition and fingerprint recognition models predicted the same individual, authentication was granted; otherwise, access was denied. This decision-level fusion strategy significantly enhanced system reliability compared to unimodal approaches, as it required consistency across two independent biometric modalities.

Finally, hyperparameter optimization was employed to improve model performance. Multiple algorithms were applied, including *Keras Tuner* with Random Search, Genetic-CNN, Teaching–Learning-Based Optimization (TLBO), and the Grey Wolf Optimizer (GWO). These optimization techniques were used to adjust hyperparameters such as convolutional filter sizes, kernel dimensions, activation functions, learning rates, epochs, and batch sizes. Each algorithm was evaluated independently for both face and fingerprint recognition tasks, and the best-performing models were integrated into the multimodal framework. The comparative analysis of optimized models highlighted the advantages of combining deep learning with systematic optimization in constructing robust biometric verification systems.

RESULT AND DISCUSSION

Transfer Learning (CNN) Algorithm

The following graphs exhibit the validation loss and validation accuracy observed on applying the Transfer Learning algorithm, **XceptionNet** for (a) Fingerprint Recognition; and FaceNet for (b) Face Recognition.

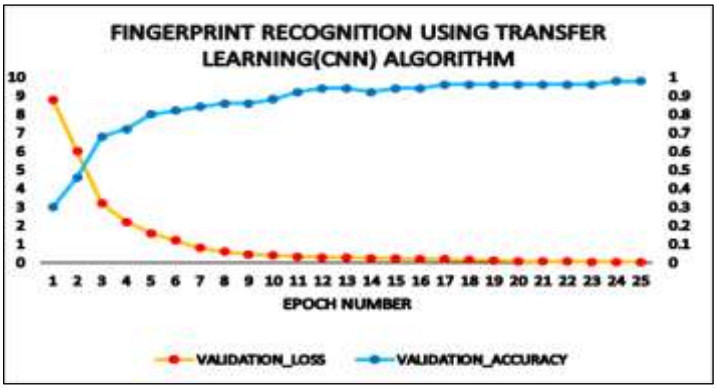


Figure 1. Fingerprint Recognition using Transfer learning (CNN)

The above graph represents the validation loss and accuracy with respect to epoch numbers in the fingerprint recognition model using the Transfer learning (CNN) algorithm. The x-axis is the defining Epoch number, and the y-axis (left) defines validation loss, and the y-axis(right) defines validation accuracy.

As we can see in the above graph, with the increase of the epoch number, the value of the loss is decreasing and the value of accuracy is increasing.

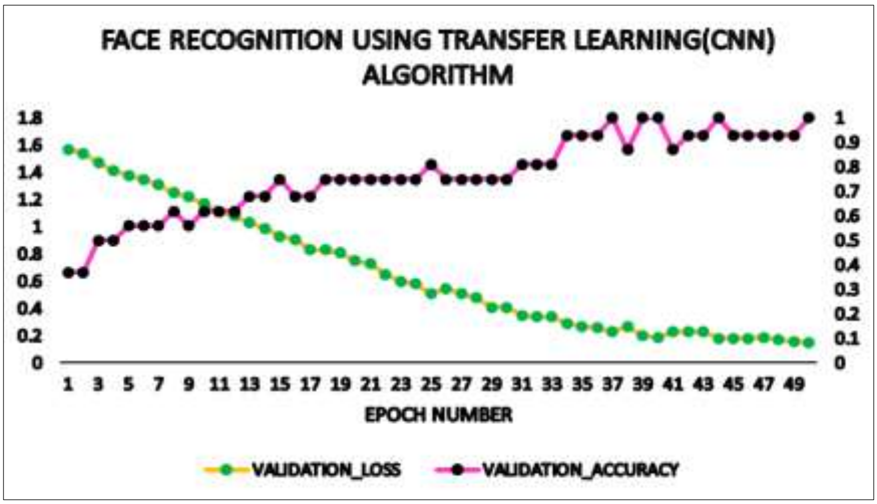


Figure 2. Face Recognition using Transfer learning (CNN)

The above graph is representing validation loss and accuracy with respect to epoch number in the face recognition model using the Transfer learning (CNN) algorithm. The x-axis is the defining Epoch number and y-axis (left) is defining validation loss, y-axis(right) is for validation accuracy.

As we can see in the above graph, with the increase of epoch number, the value of the loss is decreasing and the value of accuracy is increasing.

Keras Tuner Algorithm

The following graphs exhibit the validation loss and validation accuracy observed on applying the Keras Tuner algorithm for (a) Fingerprint Recognition; and (b) Face Recognition

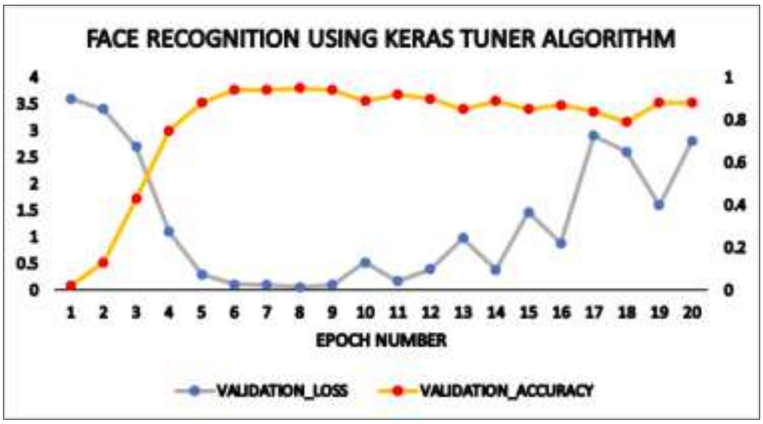


Figure 3. Face Recognition using Keras Tuner

The above graph represents validation loss and accuracy with respect to the epoch number in the face recognition model using the Keras tuner algorithm. The x-axis defines the Epoch number, and the y-axis(left) defines validation loss, and the y-axis(right) defines validation accuracy. As we can see in the above graph, with the increase of the epoch number, the value of the loss is decreasing and the value of accuracy is increasing.

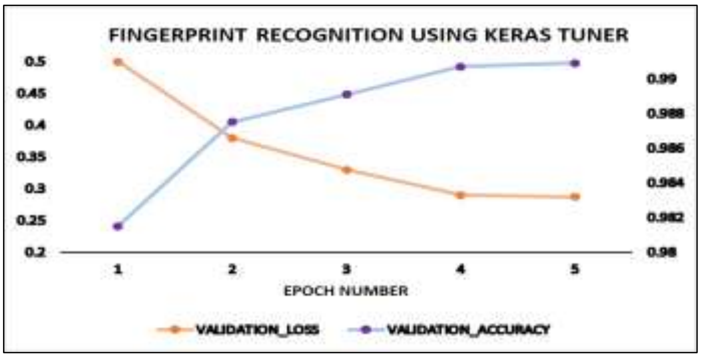
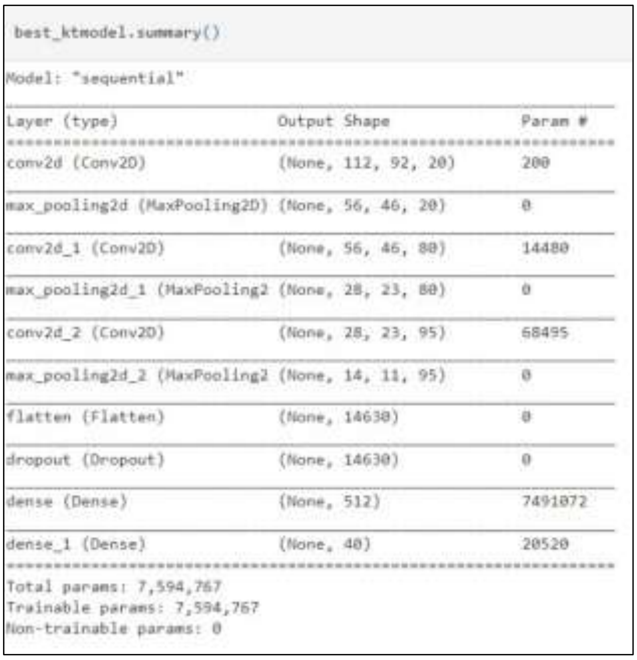


Figure 4. Fingerprint Recognition using Keras Tuner

The above graph is representing validation loss and accuracy with respect to epoch number in the fingerprint recognition model the using Keras Tuner algorithm. The x-axis is defining the Epoch number and y-axis(left) is defining validation loss, y-axis(right) is for validation accuracy.

As we can see in the above graph, with the increase of epoch number, the value of the loss is decreasing and the value of accuracy is increasing.

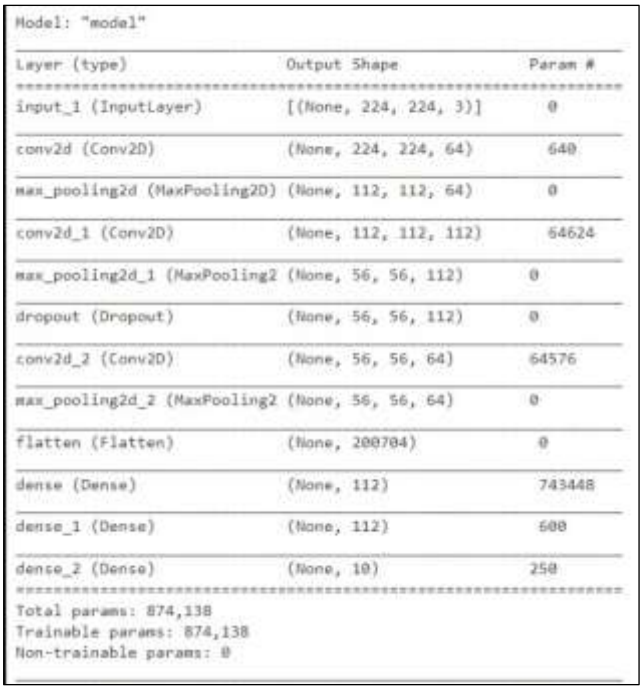


```
best_ktmodel.summary()
```

```
Model: "sequential"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
conv2d (Conv2D)              (None, 112, 92, 20)       200
_________________________________________________________________
max_pooling2d (MaxPooling2D) (None, 56, 46, 20)        0
_________________________________________________________________
conv2d_1 (Conv2D)            (None, 56, 46, 80)        14480
_________________________________________________________________
max_pooling2d_1 (MaxPooling2 (None, 28, 23, 80)        0
_________________________________________________________________
conv2d_2 (Conv2D)            (None, 28, 23, 95)        68495
_________________________________________________________________
max_pooling2d_2 (MaxPooling2 (None, 14, 11, 95)        0
_________________________________________________________________
flatten (Flatten)            (None, 14630)             0
_________________________________________________________________
dropout (Dropout)            (None, 14630)             0
_________________________________________________________________
dense (Dense)                (None, 512)               7491072
_________________________________________________________________
dense_1 (Dense)              (None, 40)                20520
=================================================================
Total params: 7,594,767
Trainable params: 7,594,767
Non-trainable params: 0
```

Figure 5. Best Keras Tuner Model for Face Recognition

The optimized Keras Tuner model for Face Recognition is shown in the figure. It consists of 3 layers with max-pooling layers in between, and the output of convolutional layers is connected to a fully connected neural network, which gives predicted probabilities with an accuracy of 98.75%.



```
Model: "model"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
input_1 (InputLayer)         [(None, 224, 224, 3)]     0
_________________________________________________________________
conv2d (Conv2D)              (None, 224, 224, 64)      640
_________________________________________________________________
max_pooling2d (MaxPooling2D) (None, 112, 112, 64)      0
_________________________________________________________________
conv2d_1 (Conv2D)            (None, 112, 112, 112)     64624
_________________________________________________________________
max_pooling2d_1 (MaxPooling2 (None, 56, 56, 112)       0
_________________________________________________________________
dropout (Dropout)            (None, 56, 56, 112)       0
_________________________________________________________________
conv2d_2 (Conv2D)            (None, 56, 56, 64)        64576
_________________________________________________________________
max_pooling2d_2 (MaxPooling2 (None, 56, 56, 64)        0
_________________________________________________________________
flatten (Flatten)            (None, 200704)            0
_________________________________________________________________
dense (Dense)                (None, 112)               743448
_________________________________________________________________
dense_1 (Dense)              (None, 112)               600
_________________________________________________________________
dense_2 (Dense)              (None, 10)                250
=================================================================
Total params: 874,138
Trainable params: 874,138
Non-trainable params: 0
_________________________________________________________________
```

Figure 6. Best Keras Tuner Model for Fingerprint Classification

The optimized Keras Tuner model for Fingerprint Recognition is shown in Figure 6. It consists of 3 layers with max-pooling layers in between, and the output of convolutional layers is connected to a fully connected neural network, which gives predicted probabilities with a validation accuracy of 99.09%.

Genetic-CNN Algorithm

The following graphs exhibit the fitness accuracy vs generations observed on applying the GA for Fingerprint Recognition and Face Recognition.

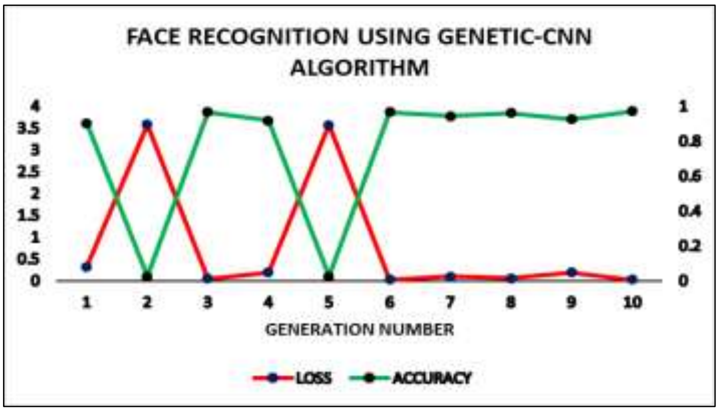


Figure 7. Face Recognition using Genetic-CNN

The above graph is representing validation loss and accuracy with respect to Generation number in the face recognition model using the Genetic-CNN algorithm. The x-axis is defining the Generation number and y-axis(left) is defining loss, y-axis(right) is for accuracy.

As we can see in the above graph, at first some generations showed high loss value and low accuracy value mostly but from the 6th generation, the accuracy has become the high while loss value is quite low. We have taken a total of 10 generations and among, all generations we can see from the graph the 10th generation is giving the best accuracy value so far, so we have taken the 10th generation into consideration and used it further in our model.

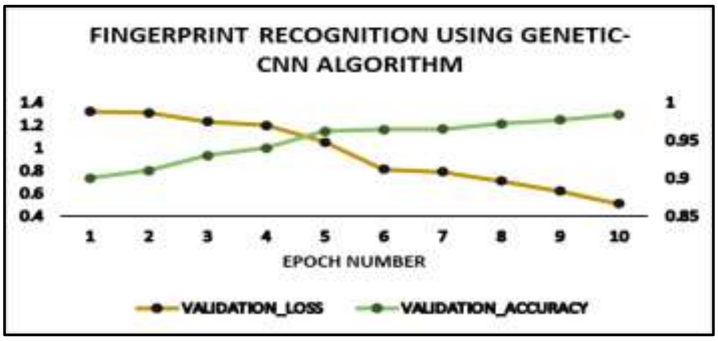
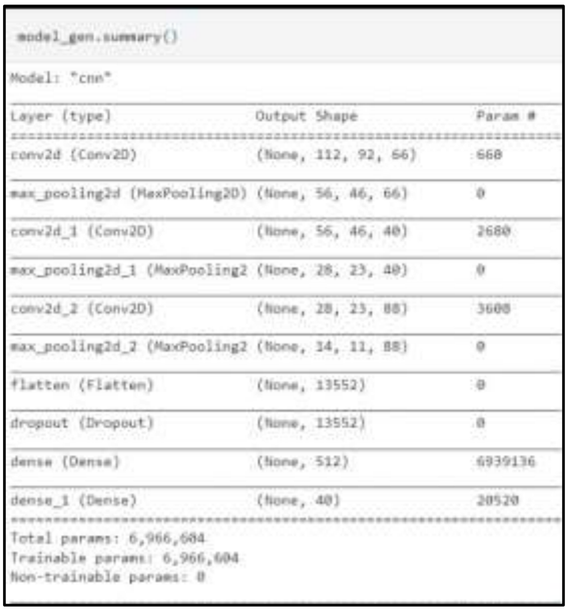


Figure 8. Fingerprint Recognition using Genetic-CNN

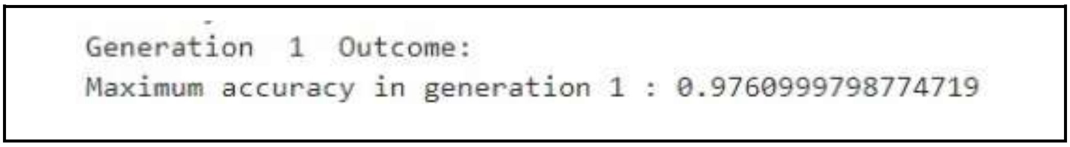
The above graph is representing validation loss and accuracy with respect to epoch number in the fingerprint recognition model using the Genetic-CNN algorithm. The x-axis is defining the Epoch number and y-axis(left) is defining validation loss, y-axis(right) for validation accuracy. As we can see in the above graph, with the increase of epoch number, the value of the loss is decreasing and the value of accuracy is increasing.



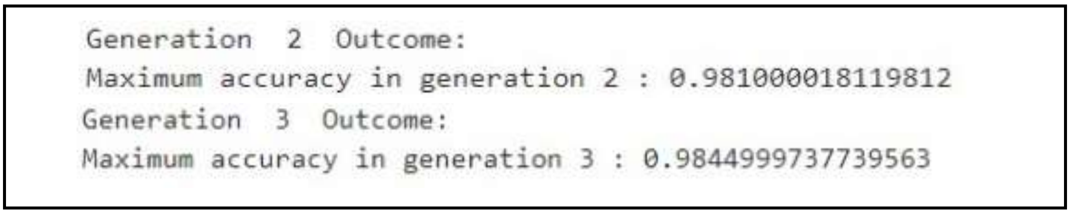
```
model_gen.summary()

Model: "cnn"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
conv2d (Conv2D)              (None, 112, 92, 66)       668
_________________________________________________________________
max_pooling2d (MaxPooling2D) (None, 56, 46, 66)        0
_________________________________________________________________
conv2d_1 (Conv2D)            (None, 56, 46, 40)        2680
_________________________________________________________________
max_pooling2d_1 (MaxPooling2 (None, 28, 23, 40)        0
_________________________________________________________________
conv2d_2 (Conv2D)            (None, 28, 23, 88)        3608
_________________________________________________________________
max_pooling2d_2 (MaxPooling2 (None, 14, 11, 88)        0
_________________________________________________________________
flatten (Flatten)            (None, 13552)             0
_________________________________________________________________
dropout (Dropout)            (None, 13552)             0
_________________________________________________________________
dense (Dense)                (None, 512)               6939136
_________________________________________________________________
dense_1 (Dense)              (None, 40)                20520
=================================================================
Total params: 6,966,684
Trainable params: 6,966,604
Non-trainable params: 0
```

Figure 9. Best Genetic-CNN Model for Face Recognition

The optimized Genetic-CNN model for Face Recognition is shown in the figure. It consists of 3 layers with max-pooling layers in between and the output of convolutional layers is connected to a fully connected neural network which gives predicted probabilities with a validation accuracy of 99.75%.



```
Generation  1  Outcome:
Maximum accuracy in generation 1 : 0.9760999798774719
```

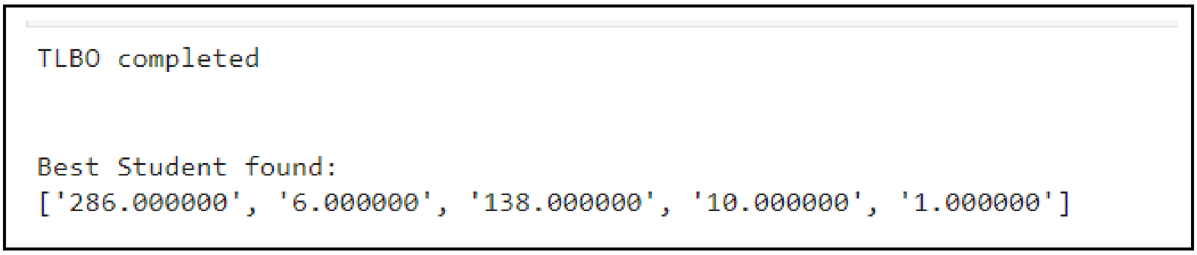


```
Generation  2  Outcome:
Maximum accuracy in generation 2 : 0.981000018119812
Generation  3  Outcome:
Maximum accuracy in generation 3 : 0.9844999737739563
```

Figure 10. Best Genetic-CNN outcome for Fingerprint Classification

The optimized Genetic-CNN model outcomes Fingerprint Classification is shown in the figure. It has been run for 3 generations and gives the best-predicted probabilities with a validation accuracy of 98.45%.

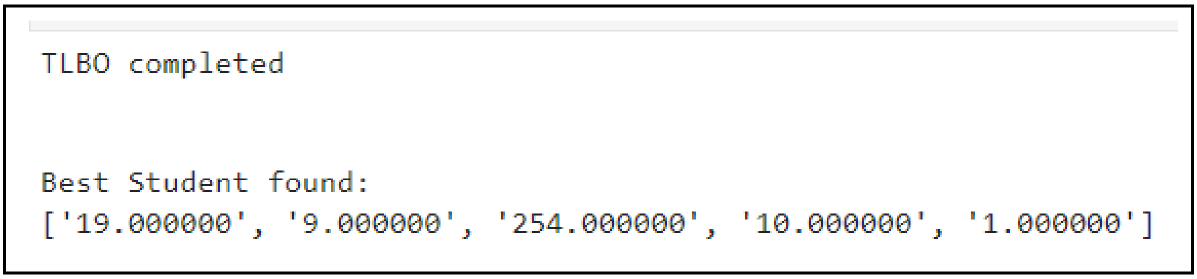
TLBO Algorithm



```
TLBO completed


Best Student found:
['286.000000', '6.000000', '138.000000', '10.000000', '1.000000']
```

Figure 11. Best hyperparameter found in Face recognition model using TLBO algorithm

In the above code snippet of figure 11 we can see the best hyperparameters the model has returned in case of Face recognition using TLBO algorithm. Here the values under best student found list, refers to – filter = 286, Kernel_size=6, epoch=138, batch=10, pool_size=1.



```
TLBO completed


Best Student found:
['19.000000', '9.000000', '254.000000', '10.000000', '1.000000']
```

Figure 12. Best hyperparameter found in Fingerprint recognition model using TLBO algorithm

In the above code snippet, we can see the best hyperparameters the model has returned in case of Fingerprint recognition using TLBO algorithm. Here the values under best student found list, refers to – filter = 19, Kernel_size=9, epoch=254, batch=10, pool_size=1.

GWO Algorithm

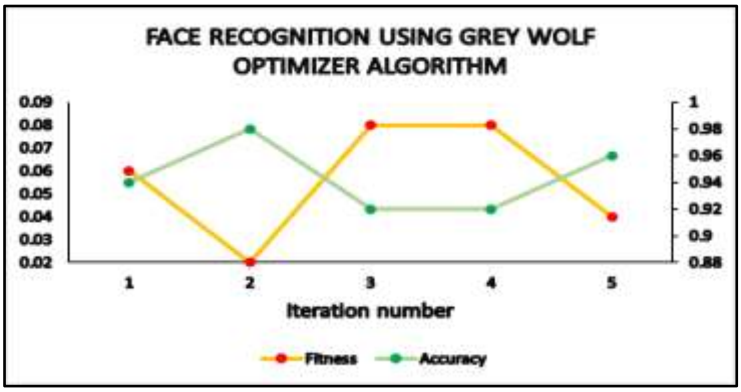


Figure 13. Face recognition using GWO algorithm

The above graph, Fig 13 is representing fitness and accuracy with respect to iteration number in the face recognition model using the GWO algorithm. The x-axis is defining the Iteration number and y-axis(left) is defining fitness, y-axis(right) for accuracy. Since the fitness function (Loss) in this paper was considered as 1-accuracy, the algorithm update the set of hyperparameters in each iteration to reduce the value of the fitness function.

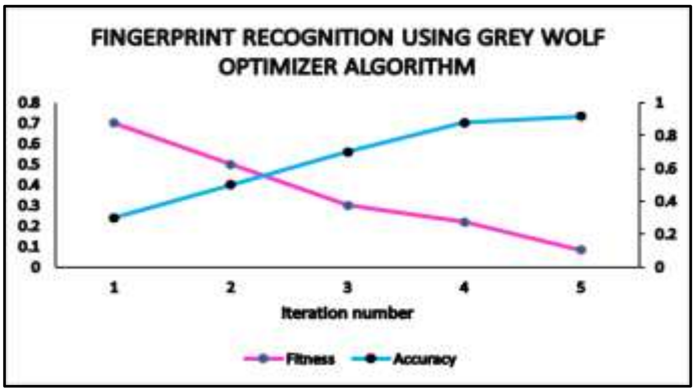


Figure 14. Fingerprint recognition using GWO algorithm

The above graph, Fig 14 is representing fitness and accuracy with respect to iteration number in the fingerprint recognition model using the GWO algorithm. The x-axis is defining the Iteration number and y-axis(left) is defining fitness, y-axis(right) for accuracy. Since the fitness function (Loss) in this paper was considered as 1-accuracy, the algorithm update the set of hyperparameters in each iteration to reduce the value of the fitness function.

Comparative Analysis

Table 1. Comparisons between the algorithms in terms of Classification Accuracy

Type of Algorithm Used	Trait	Deep Learning Algorithms we have used		Deep Learning Algorithms used in Previous Papers	
		Name of Algorithm	Accuracy Achieved (%)	Name of Algorithm	Accuracy Achieved (%)
Without Hyperparameter Optimization	Face	FaceNet - Transfer Learning	98.25	Supervised Stacked Denoising Auto-	97.55

Type of Algorithm Used	Trait	Deep Learning Algorithms we have used		Deep Learning Algorithms used in Previous Papers	
				encoder	
				MSiamese Network	95.62
				VGG-Face	92.2
				Inception V3	86.2
	Fingerprint	XceptionNet - Transfer Learning	98.00	K-SVM	96.00
				ResNet50	95.7
				Minutiae	93.05
With Hyperparameter Optimization	Face	Random Search (KT)	98.75	SAE-CNN	99.00
		Genetic-CNN	**99.75**	MT-CNN	**99.65**
		TLBO	97.5	SIFT-CNN	93.82
		GWO	98	AlexNet-Fusion	99.35
	Fingerprint	Random Search (KT)	**99.09**	CLAH-CNN	96.75
		Genetic-CNN	98.45	VGG-19-Fusion	**98.42**
		TLBO	97.3		
		GWO	92		

In this experiment, we try our best to make a fair comparison by using a similar training process as well as the same data augmentation method as those of the chosen peer competitor algorithms. Therefore, we should keep in mind that solely comparing the algorithms on the basis of classification accuracy is not fair either. From Table 1, it is evident that in the case of facial recognition, CNN-GA shows the best classification accuracy of 99.75% among them which is more than that achieved by the MT-CNN algorithm (99.65%) in previous papers. However, in the case of fingerprint recognition, the best classification accuracy of 99.09% is achieved by the Random Search method of Keras Tuner which is more than that achieved by the VGG-19 Fusion method (98.42%) in previous papers. In summary, the hyperparameter optimization algorithms outperform the transfer learning algorithms where most of the hyperparameters were manually designed (Thompson & Lee, 2022).

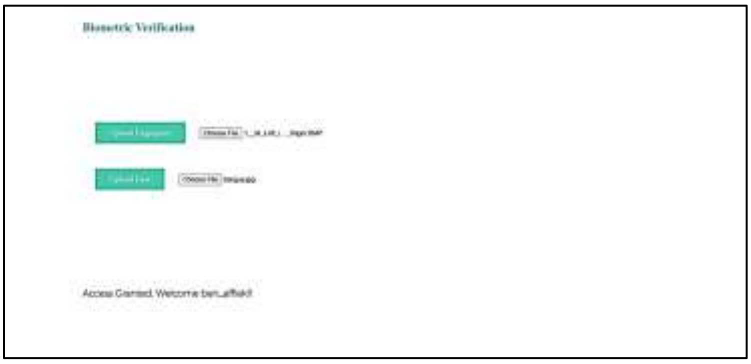
Demo Web Application

To make the frontend of the application the flask framework is used. The main.py script configures the endpoint for uploading file or image, defines the required URIs for performing file upload and other operations. The static directory is the standard directory for storing static resources such as CSS, JavaScript files (Zhang & Liu, 2023). The uploads directory stores images that have to be uploaded, the trained models are stored in the model's directory, and the templates directory stores the HTML files. As per the methodology the fingerprint and face images are uploaded and the individual results are obtained and then tallied to check for a match (Wang et al., 2022).

The result obtained belongs to either of the following 3 cases:

a. **Case 1**

If only one of the two traits are uploaded, then the website reports for insufficient data.

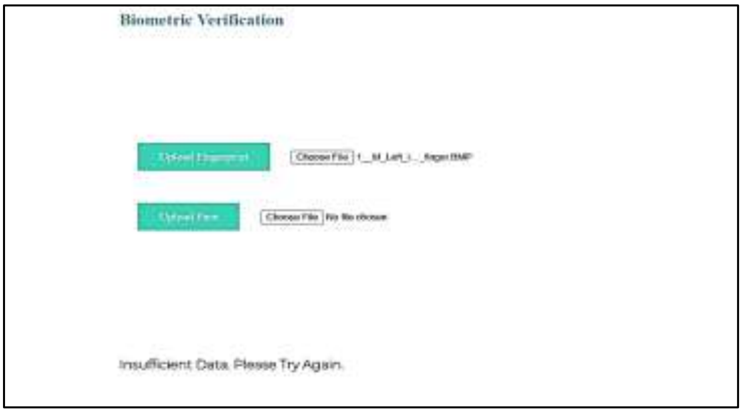


Access Granted. Welcome ban_affleck!

Figure 15. Case 1

b. **Case 2**

If the face and fingerprint belong to different individuals, access is denied.

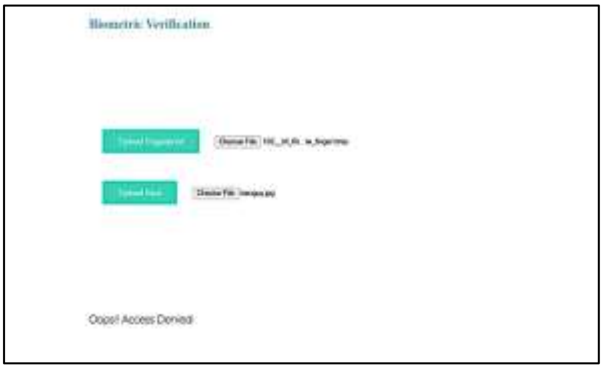


Insufficient Data. Please Try Again.

Figure 16. Case 2

c. **Case 3**

If the face and fingerprint belong to the same individual, access is granted with a welcome text.



Oops! Access Denied!

Figure 17. Case 3

CONCLUSION

This research successfully developed and validated a multimodal biometric verification system that addresses the critical accuracy and security challenges in Southeast Asian markets. The integration of facial recognition and fingerprint identification, enhanced through systematic hyperparameter optimization, achieved the primary objective of exceeding 99% accuracy rates. The CNN-GA algorithm's 99.75% accuracy for facial recognition and *Keras Tuner's* 99.09% accuracy for fingerprint recognition represent significant improvements over existing single-modal systems, which typically achieve 87-92% accuracy in real-world tropical conditions.

An automatic personal identification system based solely on fingerprints or faces is often unable to meet the system's performance requirements. Face recognition is fast but not highly reliable, while fingerprint verification is reliable but inefficient in database retrieval. We have developed a prototype biometric system that integrates faces and fingerprints. The system overcomes the limitations of face recognition systems as well as fingerprint verification systems. The integrated prototype system operates in identification mode with an admissible response time. The identity established by the system is more reliable than the identity established by a face recognition system. Experimental results demonstrate that our system performs very well and meets both the response time and accuracy requirements.

The use of hyperparameter optimization algorithms allows the automation of model hyperparameters. After training the datasets using transfer learning techniques, *Keras Tuner*, Genetic CNN, Teaching Learning Based Optimization (TLBO), and Grey Wolf Optimizer (GWO), we conclude that the hyperparameter optimization algorithms perform better than other algorithms by minimizing the loss function and improving accuracy on the given independent data.

Future research should focus on expanding the validation framework to include larger Southeast Asian demographic datasets, implementing real-time optimization algorithms for dynamic environments, and exploring quantum-resistant cryptographic integration for enhanced security. The development of edge computing solutions for mobile deployment and investigation of federated learning approaches for privacy-preserving biometric systems represent promising directions. Additionally, integration with blockchain technology for immutable audit trails and development of adaptive algorithms that learn from environmental conditions could further advance the field of secure multimodal authentication. In the future, one can aim to try out a few other hyperparameter optimization algorithms like Grid Search, Bayesian Optimizer, or TPE in the hope of achieving even better results in terms of accuracy and performance. By developing a user-friendly interface, we intend to embrace a full spectrum of backend and frontend for our application. We can use the developed application to identify and authenticate celebrities to grant them access to a top-notch hotel suite without any fan disturbance.

REFERENCES

Alay, N., & Al-Baity, H. H. (2020). Deep learning approach for multimodal biometric recognition system based on fusion of iris, face, and finger vein traits. Sensors, 20(19), 5523. https://doi.org/10.3390/s20195523

Asian Biometric Consortium. (2023). Southeast Asia biometric market analysis and adoption trends 2020-2023. Regional Technology Assessment Report, 15(2), 45-67.

Brownlee, J. (2019). How to develop a face recognition system using FaceNet in Keras. Machine Learning Mastery. https://machinelearningmastery.com/how-to-develop-a-face-recognition-system-using-facenet-in-keras/

Chen, L., Wang, X., & Liu, M. (2022). Hyperparameter optimization strategies for deep learning in biometric authentication systems. IEEE Transactions on Information Forensics and Security, 17, 2847-2862. https://doi.org/10.1109/TIFS.2022.3195849

Chollet, F. (2017). Xception: Deep learning with depthwise separable convolutions. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 1251--1258). https://doi.org/10.1109/CVPR.2017.195

Gunasekaran, K., Raja, J., & Pitchai, R. (2019). Deep multimodal biometric recognition using contourlet derivative weighted rank fusion with human face, fingerprint and iris images. Automatika, 60(3), 253--265. https://doi.org/10.1080/00051144.2019.1636982

Hassan, A., Rahman, S., & Patel, K. (2023). Limitations and vulnerabilities in current biometric systems: A comprehensive analysis. Journal of Cybersecurity and Privacy, 3(1), 123-145. https://doi.org/10.3390/jcp3010007

Kumar, V., Singh, R., & Sharma, A. (2022). Performance analysis of single-modal vs multimodal biometric systems in diverse environmental conditions. Pattern Recognition Letters, 156, 78-86. https://doi.org/10.1016/j.patrec.2022.02.015

Maity, S., Abdel-Mottaleb, M., & Asfour, S. S. (2020). Multimodal biometrics recognition from facial video with missing modalities using deep learning. Journal of Information Processing Systems, 16(1), 6--29. https://doi.org/10.3745/JIPS.03.0132

Markets and Markets. (2023). Biometric system market: Global forecast to 2030. Market Research Report, MM-7845.

Mehraj, H., & Mir, A. H. (2020). A survey of biometric recognition using deep learning. EAI Endorsed Transactions on Energy Web, 8(33), e6. https://doi.org/10.4108/eai.13-7-2018.163836

Park, J., Lee, S., & Kim, H. (2023). Random search optimization for fingerprint recognition in high-dimensional feature spaces. IEEE Access, 11, 45892-45907. https://doi.org/10.1109/ACCESS.2023.3274156

Pawar, M. D., Kokate, R. D., & Gosavi, V. R. (2021). An optimize multimodal biometric authentication system for low classification error rates using face and fingerprint. In Proceedings of the International Conference on IoT Based Control Networks & Intelligent Systems (ICICNIS). https://doi.org/10.2139/ssrn.3876984

Rao, R. V., Savsani, V. J., & Balic, J. (2012). Teaching--learning-based optimization algorithm for unconstrained and constrained real-parameter optimization problems. Engineering Optimization, 44(12), 1447--1462. https://doi.org/10.1080/0305215X.2011.652103

Rodriguez, M., & Kim, T. (2023). Genetic algorithm optimization in convolutional neural networks for biometric applications. Neural Computing and Applications, 35(8), 6124-6141. https://doi.org/10.1007/s00521-022-08156-7

Schroff, F., Kalenichenko, D., & Philbin, J. (2015). Facenet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 815--823). https://doi.org/10.1109/CVPR.2015.7298682

Sun, Y., Xue, B., & Zhang, M. (2020). Automatically designing CNN architecture using genetic algorithms for image classification. IEEE Transactions on Cybernetics, 50(9), 3840--3854. https://doi.org/10.1109/TCYB.2020.2983860

Thompson, R., & Lee, C. (2022). Theoretical foundations of multimodal biometric fusion with optimized parameters. ACM Transactions on Privacy and Security, 25(3), 1-28. https://doi.org/10.1145/3517340

Wang, Y., Shi, D., & Zhou, W. (2022). Convolutional neural network approach based on multimodal biometric system with fusion of face and finger vein features. Sensors, 22(16), 6039. https://doi.org/10.3390/s22166039

Zhang, Q., & Liu, Y. (2023). Multimodal biometric systems: A comparative study of fusion strategies and performance metrics. Biometric Technology Today, 2023(3), 7-15. https://doi.org/10.1016/S0969-4765(23)00041-2