LAUTECH Journal of Engineering and Technology 20 (1) 2026: 290-299
10.36108/laujet/6202.02.0142

Experimental Recognition Performance of CO with CNN on Handwritten Signature at Optimal Threshold

[1*]Ayangbekun O. J., [2]Oladosu J. B., [2]Falohun A. S., [2]Awodoye O. O., [2]Ige B. O.

[1] *Department of Computer Engineering, Federal Polytechnic Ayede, Oyo State. Nigeria.*
[2]*Department of Computer Engineering, Ladoke Akintola University of Technology, Ogbomoso. Oyo State, Nigeria.*

Article Info

Article history:

Received: Dec 31, 2025
Revised: Feb 01, 2026
Accepted: May 07, 2026

Keywords:

Handwritten Signature Recognition, Cheetah Optimization Algorithm, Convolutional Neural Network, Biometric Authentication, Deep Learning Optimization, Signature Verification

Corresponding Author:
ayangbekunoj@federalpolyayde.edu.ng

ABSTRACT

The issue of identity recognition using handwritten signature biometrics features has been an important aspect in day-to-day human activities. Recurring disparities in signature recognition and identification system sprouts out greatest challenge due to health instability status, mood and uprising imitations initiated by forgers. In image processing tasks, CNN has been the prominent baseline deep learning architecture for image recognition and classification. Despite this, certain inadequacies were still identified in CNN model, which includes overfitting, hyperparameter tuning, and recognition accuracy. This calls for optimizing the CNN parameters using Cheetah Optimization (CO) algorithm for better performance. In this research, 5220 signature datasets were acquired; comprising 2750 genuine and 2470 forged signature samples. The image datasets were simulated with MATLAB R2023a and evaluated using Confusion Matrix six evaluation metrics - False Positive Rate (FPR), Precision, Sensitivity, Specificity, Accuracy and Recognition Time. At optimal threshold values of 0.75 for the two models (CNN and CO-CNN), mathematical equations were derived to affirm the model's correlation using curve-fitting tools in MS Excel to depict the systems performance. For recognition time (R_T) analysis, the complexity associated with CO-CNN is less than that of CNN thereby improving the balance between the exploration and exploitation stage of the technique. In terms of Precision, Specificity, Accuracy and recognition Time performance metrics, CNN produced 95.66%, 96.11%, 95.84% at 211.12secs respectively whereas CO-CNN produced 96.92%, 97.24%, 97.03% and 168.27secs respectively. In general, the overall results indicate that application of Cheetah optimization algorithm to CNN enhances the model's performance.

INTRODUCTION

Signature refers to a handwritten representation of someone's name, nickname, or distinctive marks, which an individual creates, draws, or writes on documents to establish their identity and intentions. The person who writes the signature is commonly known as the signatory or signer. The act of signing is widely recognized as a valid and customary way to verify distinct identity. Throughout history, individuals worldwide had been making use of signatures for authentication reasons in various aspects of their daily lives, including banking, legal agreements, and other activities. Typically, a signature entails a mixture of unique letterings and personality's name. This is often inscribed in a distinct manner and may sometimes appear in an illegible form (Iranmanesh et al., 2014; Sharif et al., 2020).

However, the availability of many and varied real-world signature datasets is one of the major obstacles, even though deep learning models have shown considerable promise in a variety of image identification and verification tasks, including signature detection. The vast variety of authentic signatures and their forgeries may not be well captured by so many recent researches due to very limited and constrained datasets. The investigation of methods to produce or get access to larger, more representative datasets for training and assessing deep learning models for signature identification represents research need; as signature forgers are always coming up with new ways to trick identification algorithms.

Existing models may not entirely solve this problem, which makes it difficult to recognise signatures from people with different writing styles. Deep learning models that can tolerate inter-writer variability and adapt to various signature styles must be developed by research. Nevertheless, research on methods to manage online and dynamic signatures using CNNs may have applications in the real world; as the styles of handwritten signatures vary widely, and some people's signatures may change dramatically over time.

This creates a vacuum in terms of research gap that requires attention with deep learning models' capacity to adapt to such a wide variety of data. This brought about this research applying Cheetah Optimizer (CO) algorithm innovative architecture on Convolutional Neural Network (CNN) in enhancing the performance on signature forgery detection and recognition through optimized CNN architecture (Atanda et al., 2023, Oguntoye et al., 2023).

In conclusion, the existing a research gap on how to handle such signature variability in CNN-based systems by filling up these knowledge gaps, leads to an optimized CNN models using Cheetah algorithm for fraudulent handwritten-signature recognition systems development offering improved security and authentication across a variety of applications; to provide an optimal solution.

LITERATURE REVIEW

Signature Verification and Validation

Tackling the challenges being encountered in signature verification and validation system, deep learning algorithm have shown prominence in terms of better performance (Ayangbekun et al., 2026). Deep learning techniques with custom feature extraction algorithms make up the two types of automatic offline signature verification solutions. These techniques in particular are seen as the most promising way among them because of their exceptional potential for picture identification and detection. Although recent research has demonstrated a great deal of interest in using deep learning with small-scale data, but majority of deep-learning approaches need a large number of samples to successfully train their systems. Therefore, in order to efficiently complete the training process for the sets of data, several signature models are required (Kao and Wen, 2020; Akintunde et al., 2025).

Meanwhile, one of the most effective baseline models in deep learning for signature verification is Convolutional Neural Networks (CNNs) being principally effective for image detection, classifications and signal processing tasks. CNN have achieved impressive success in various tasks related to image recognition and classification. They have also demonstrated significant potential in medical imaging analysis, particularly in predicting brain tumors. CNNs possess the ability to automatically learn relevant features from input images, making them well-suited for detecting intricate patterns in medical data (Ogundepo et al., 2022). Recent state-of-the-art literature in deep learning applications reveals that CNNs are extensively utilized for diverse image classification and segmentation tasks within the medical domain (Xuxin et al., 2022). However, CNN still faces overfitting problem, hyperparameters tunning and premature convergence. This calls for optimization of parameters using metaheuristics algorithm (Adetunji et al., 2015, Adetunji et al., 2018, Oguntoye et al., 2025).

RELATED WORKS

Abdelrahman and Abdallah (2013) proposed a support vector machine-based offline signature verification system. Using the Radon transform, they were able to extract global characteristics from the signatures. Different reference signatures are chosen and changed for each enrolled client in the system's database in order to obtain insightful data about the signature. Two signatures were aligned using a dynamic time-warping approach, and different real and fake signatures were selected for the training of the support vector machine classifier. By lining up the test signature with each reference signature for the claimed identity, they created a test signature verification. The signature was then classified as authentic or fake. The suggested approach, however, is constrained by the fact that it only makes use of the global characteristics that the radon transforms extracts from the signatures. This might lead to a restricted ability to distinguish between real and fake signatures.

Shrivastava (2016) put forth a Support Vector Machine (SVM)-based offline signature identification method and used the Gabor filter and Discrete wavelet transform to extract signature characteristics. Their suggested methods are divided into three sections: preprocessing, feature verification, and the third section involves designing a signature verification system using SVM to recognise signatures. The study's use of a single feature extraction technique, and SVM's performance was not compared to that of other classifiers, which may have shown if SVM was the right solution for the issue. Choosing filter parameters like the Gabor filter's size and orientation have a big impact on how well features are extracted. It may be difficult to find the best values for these factors and may need professional understanding of the data. The findings were evaluated in Matlab 2012 with 110 signatures of 10 persons (small number of datasets) with quantitative experimental results of up to 80-85% recognition rate thereby asserting an improved signature recognition accuracy.

Sharma, N., Gupta, S., & Mehta, P. (2021) transformed the signature picture into time series data using a linear scanning approach to discriminate between real and false signatures. The scale-invariant Mahalanobis distance metric, which takes into account the correlation of the data points, was employed by the researchers to compare the time series data. The experiment's findings demonstrated that the proposed technique significantly lowered the rate of equal mistakes. The linear scanning approach, however, may not be appropriate for signatures with intricate forms or overlapping strokes. However, the covariance matrix must be reliably estimated using numerous training samples, which may be computationally costly, and may not be practical in certain cases, and may not function well for data that cannot be separated linearly. The experiments are conducted on dataset containing 1287 questioned signatures and 646 reference signatures. The method showed 5.8% Equal Error Rate (EER) indicating a great reduction in Error Rate in terms of classification time series. Summra et al. (2021) used an artificial neural network built on the well-known Backpropagation technique; y presenting a label that shows how similar the signature under study and the original signature are. The method made advantage of the neural network's ability to distinguish patterns and extract characteristics. To evaluate the efficiency of the method, the researcher examined 400 signature samples, which included genuine and counterfeit signatures from 20 individuals. They then computed the Equal Error Rate (EER), False Reject Rate, and False Accept Rate. When training on huge datasets, the Backpropagation technique was sluggish and took a while to converge; thereby being caught in local minima during training, missing the global minimum and producing less-than-ideal solutions. Experimental results were provided for the training and performance evaluation with 900 signatures collected from various sources to train the system. The quantitative results produce 0.177 error rate, equal error rate (EER) value of 33%, False Reject Rate (FRR) of 0.04 and False Accept Rate (FAR) of 0.08. Hence the experimental results for the accuracy, speed and throughput showed excellent measurements that are comparable to the benchmark algorithms in the domain. Sathya, et al (2022) presented an autonomous offline method for signature verification and fraud detection. Various characteristics were retrieved, and their impact on the capacity of the system to recognise objects was reported. Run length distributions, slant distributions, entropy, Histogram of Gradients features (HOG), and geometric features are some of the calculated characteristics. Finally, the calculated features were subjected to the application of several machine learning algorithms, including Support Vector Machine (SVM), Random Forest, and Bagging Tree. When used on HOG features, SVM was shown to perform better than the other classifiers. Measuring the performance of SVM, bagging trees and Random Forest classifiers using different types of features indicates that SVM outperforms the other two classifiers: bagging tree and random forest. Support vector machine (SVM) classifier achieves the best accuracy, which is 94% in detecting forgery in signatures. Random Forest - 86% and Bagging Trees - 79.7 % accuracy level. Possible.

METHODOLOGY

Datasets Signatures collection

A total set of 5220 signatures comprises of genuine and forged signatures were acquired. 275 genuine signatures were collected with 10 samples from each of the signers. On the other hand, 247 forged signatures were collected from people with each of the signers signing 10 times each (Table 1).

Table 1. Signatures Collection

	Signers	No. of samples	Total Number
Genuine Signatures	275	10	2750
Forged Signatures	247	10	2470

Software and Hardware requirements

User-friendly Graphic User Interface (GUI) application will be created, incorporating a Local Database containing digital images of handwritten signatures. The GUI design will leverage toolboxes such as image processing, deep learning, and optimization within MATLAB 2023a framework. The implementation will be carried out using the MATLAB software package on a computer system with Windows 11 64-bit operating system, x64-based processor 13th Gen Intel(R) Core (TM) i7-1355U (1.70 GHz) and 16GB of RAM hardware configuration.

Research Paradigm

The procedural model description for the signature datasets / images passes through diverse stages. It began from datasets acquisition stage to pre-processing stage, feature extraction, image segmentation and performance evaluation stage (Figure 1). 5220 signature samples were acquired in this research out of which 2750 were classified as genuine and 2470 as forged. A randomized sub-sampling cross-validation approach will be applied, with 70% of the dataset allocated for training and 20% for testing and 10% for validation to ensure generalized learning Image pre-processing phase train and test the sets of acquired data. This is crucial for enhancing the quality of handwritten signature images, removing noise, and extracting relevant features for verification or recognition. To achieve feature extraction of preprocessed images, binary conversion and thresholding; Denoising and Image Enhancement will be carried out. Feature extraction stage plays an important role in any recognition process to shape the input images in a form suitable for segmentation. The image segmentation completely isolates signature images from the background, extracting bounding boxes or contours and other artifacts such as Image Resizing and Border Removal from the signature (Figure 1).

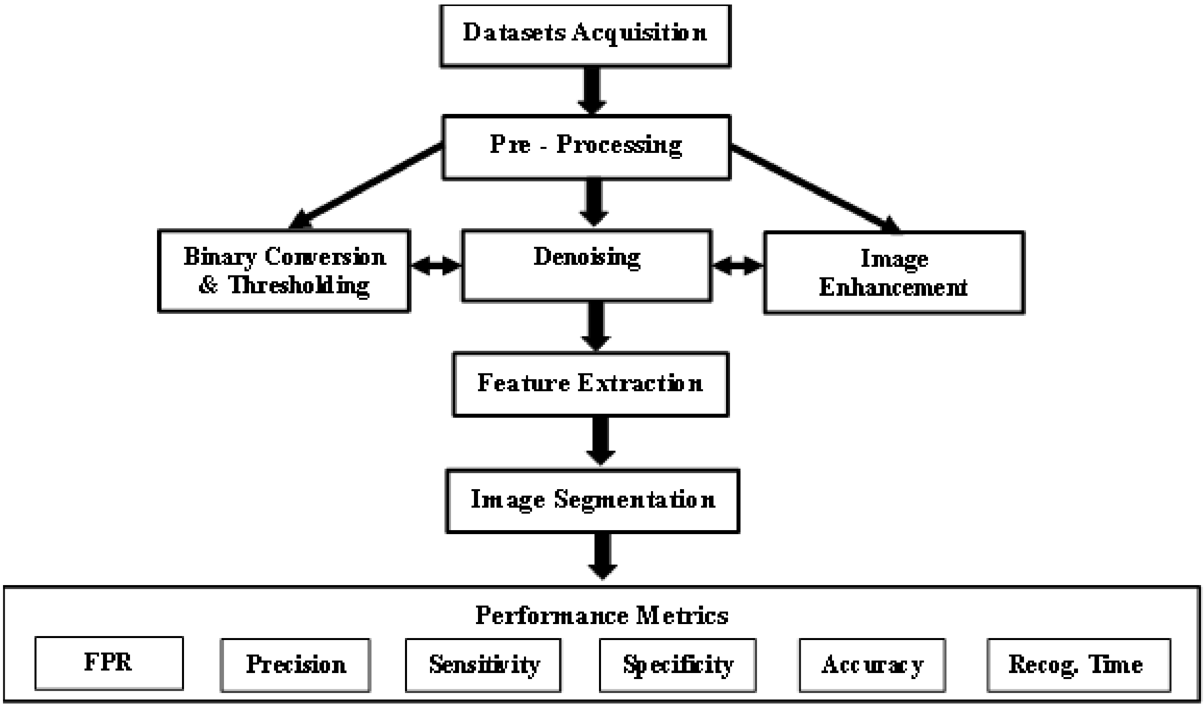

Figure 1. Performance Procedural model

The signature datasets are then simulated using MATLAB R2023a for performance evaluation based on the confusion matrix metrics.

Model Performance Metrics

Evaluation of CO-CNN model performance is implemented using MATLAB 2023a using six-performance metrics: False Positive Rate (FPR), Precision, Sensitivity, Specificity, Accuracy and Recognition Time (Table 2). In this context, correctly identified foregrounds are termed as true positives (TP), while undetected foregrounds are referred to as false negatives (FN). Objects falsely identified are labeled as false positives (FP), and true negatives (TN) denote objects not incorrectly identified.

RESULTS AND DISCUSSION OF FINDINGS

Metrics Results Analysis

System simulation involving training, testing and classifications were based on the acquired datasets of 2750 Genuine signatures and 2470 forged signatures (Table 3).

Table 2. Metrics Description

S/N	METRICS	MATHEMATICAL EXPRESSION	DEFINITION	REQUIREMENTS
1.	False Positive Rate (FPR)	$\frac{\text{FP}}{\text{TN} + \text{FP}} X\,100$	Percentage of genuine signatures incorrectly identified as forgeries by a verification system	Lower FPR indicates better performance
2.	Precision	$\frac{\text{TP}}{\text{TP} + \text{FP}} X\,100$	The accuracy of a signature verification system in correctly identifying genuine signatures as authentic	Higher precision indicates better performance
3.	Sensitivity	$\frac{\text{TP}}{\text{TP} + \text{FN}} X\,100$	Ability of a signature verification system to correctly identify genuine signatures as authentic	Higher sensitivity indicates better performance
4.	Specificity	$\frac{\text{TN}}{\text{TN} + \text{FP}} X\,100$	Ability of a signature verification system to correctly identify forgeries as fake (the proportion of detected forgeries).	Higher specificity indicates better performance
5.	Accuracy	$\frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} X\,100$	Percentage of correctly classified signatures (both genuine and forged) by a signature verification system	Higher accuracy indicates better performance
6.	Recognition Time	$\frac{\text{No. of Ident handwritten sign}}{\text{Total No. of ident H/written sign}} X\,Ti$	Time taken by a signature verification system to process and verify a signature.	Lower computation time indicates better performance

Table 3. Datasets Classifications

GENUINE SIGNATURE	FORGED SIGNATURE	TOTAL
2750	2470	5220

The simulation analysis were separately performed on the two models (CNN and CO-CNN) as shown in Figure 2.

The analysed performance metrics (False Positive Rate (FPR), Precision, Sensitivity, Specificity, Accuracy and Recognition Time) were subjected to threshold of 0.25, 0.35, 0.45 and 0.75 ranging from 0-0.25, 0.26-0.35, 0.36-0.45 and 0.46-0.75 respectively.

Table 4. Performance of the CNN technique on signature Image Dataset

Threshold	TP	FN	FP	TN	FPR (%)	PREC (%)	SEN (%)	SPEC (%)	ACC (%)	Time (sec)
0.25	2363	107	114	2636	4.15	95.40	95.67	95.85	95.77	212.46
0.35	2362	108	112	2638	4.07	95.47	95.63	95.93	95.79	212.43
0.45	2361	109	110	2640	4.00	95.55	95.59	96.00	95.80	210.00
0.75	2360	110	107	2643	3.89	95.66	95.55	96.11	95.84	211.12

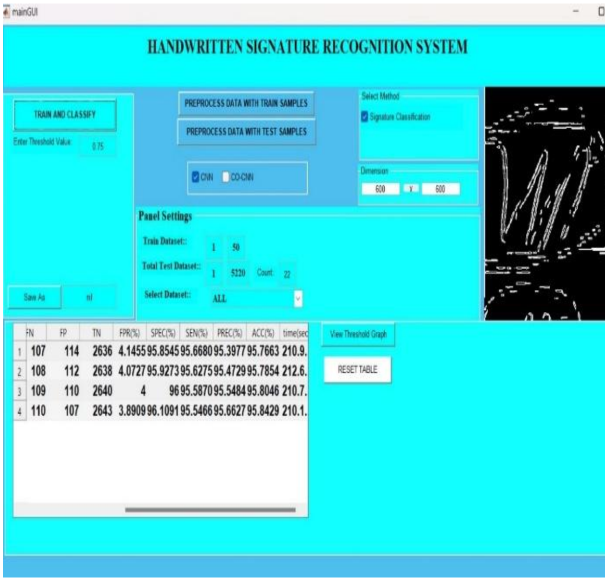

Figure 2. Simulation Process

CNN Analysis

Based on 5220 acquired signature datasets simulation, Table 4 presented the result obtained by the CNN technique at different threshold values with respect to the performance metrics. The optimal performance were obtained at 0.75 threshold values.

CO-CNN Analysis

In this case, the cheetah Algorithm was applied to optimize CNN hyperparameters. The outcomes attained through the CO-CNN technique at various threshold values, focusing on performance metrics, are indicated in Table 5 with the optimal performance at 0.75 threshold value.

Table 5. Performance of the CO-CNN technique on signature Image Dataset

	TP	FN	FP	TN	FPR (%)	PREC (%)	SEN (%)	SPEC (%)	ACC (%)	Time (sec)
0.25	2394	76	84	2666	3.05	96.61	96.92	96.95	the	176.66
0.35	2393	77	81	2669	2.95	96.73	96.88	97.05	96.97	179.34
0.45	2392	78	78	2672	2.84	96.84	96.84	97.16	97.01	171.93
0.75	2391	79	76	2674	2.76	96.92	96.80	97.24	97.03	168.27

Considering the above metrics results analysis, CO-CNN technique has a lower recognition time of 168.27secs compared with the corresponding CNN technique at 211.12secs. Also, in terms of accuracy, CO-CNN produces 97.03% compared with 95.84% for CNN. The graphical threshold representation in terms of the model accuracy at threshold values is shown in Figure 2 with changes at 0.26, 0.36 and 0.46 threshold values (Figure 3).

Experimental Recognition Time Analytical Evaluation

The computation time attained by the CO technique with threshold values between 0.25 and 0.75 is shown in Table 6 and that of the CO-CNN technique is represented in Table 6. The relationship between the CNN and CO-CNN approach based on total recognition time is shown in Figure 4. The indicated graph illustrates how the threshold values (th) and recognition time (R_T) for the signature identification system correlate with one another. According to equation 1, the relationship was determined to be quadratic with a high correlation coefficient for the CO-CNN technique and equation 2 established the relationship in terms of recognition time with respect to the threshold values to be a polynomial of the third order with a high correlation coefficient in both CNN and CO-CNN techniques.

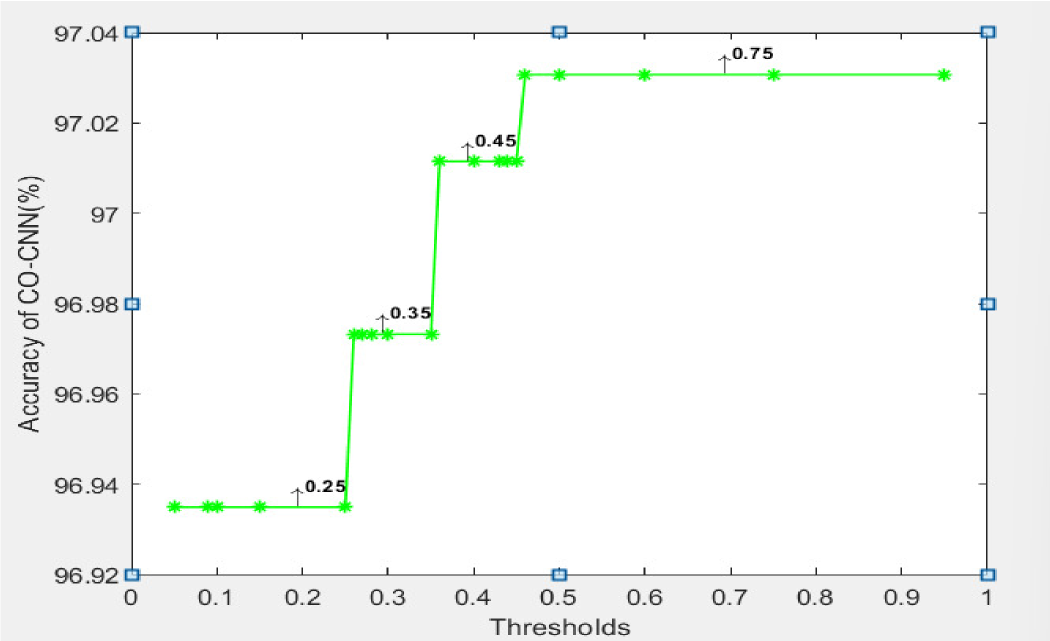

Figure 3. Thresholds Accuracy Evaluation Graph

Table 6. Model's computation Time at threshold values

Threshold	0.25	0.35	0.45	0.75
CNN	212.46	212.43	210.00	211.12
CO-CNN	176.66	179.34	171.93	168.27

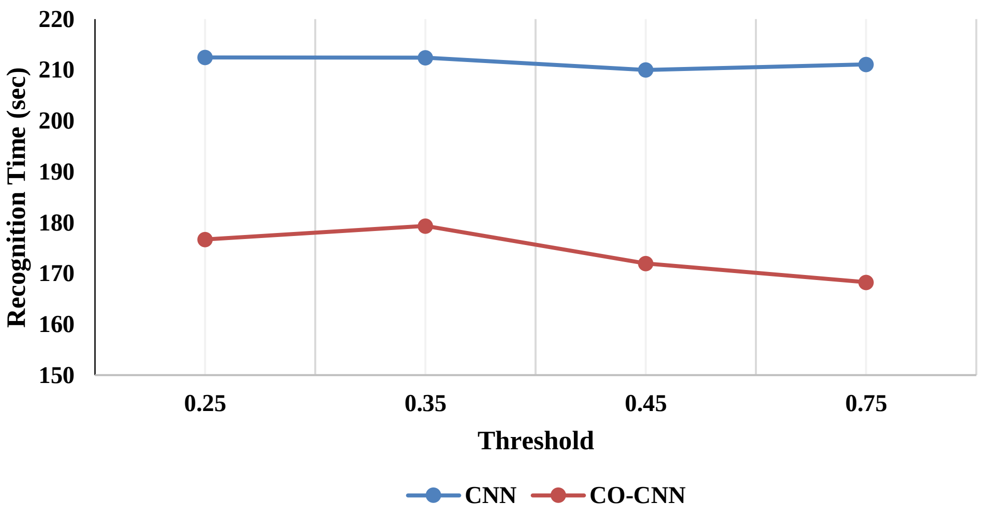

Figure 4. Relationship between Recognition Time (R_T) and Threshold (*th*)

For CO-CNN,

$R_T = 24.982th^2 - 28.551th + 218.42 \quad R^2 = 0.6568 \quad (1)$

For Both CNN and CO-CNN,

$R_T = 1318.6th^3 - 1888.9th^2 + 800.75th + 73.928 \quad R^2 = 1 \quad (2)$

As demonstrated, the CNN technique has a time complexity of $O(n^3)$ while the CO-CNN technique has a time complexity of $O(n^2)$, as evidenced based on the recognition time's performance with regard to the threshold (th) values in both techniques. As a result, time complexity is decreased by the created CO approach. Considering the comparative analysis of both techniques, the optimization of the CNN parameters by CO had contributed immensely by improving the recognition percentage and reduced computational time.

CONCLUSION

Obviously, in terms of recognition time analysis, the experimental results revealed that the CO-CNN technique takes less time for recognition compared to CNN. This establishes that the time complexity associated with CO-CNN is less than that of CNN for the signature recognition system. The reduction in the recognition time achieved by the CO-CNN technique is because of the introduction of CO to CNN, which improves the balance between the exploration and exploitation stages of the technique.

ACKNOWLEDGEMENT

The authors wish to thank the Federal Ministry of Education, Nigeria, through the TETFUND Institution-Based Research (IBR) Intervention funding for sponsorship.

REFERENCES

Abdelrahman, A., & Abdallah, A. (2013). Signature verification system based on support vector machine classifier. *The international Arab conference on information technology (ACIT'2013)*, Vol. 6.

Adetunji, A. B., Oguntoye, J. P., Fenwa, O. D., & Omidiora, E. O. (2018). Reducing the computational cost of SVM in face recognition application using hybrid cultural algorithm. *IOSR Journal of Computer Engineering (IOSR-JCE)*, *20*(2), 36-45.

Akintunde, O. A., Adetunji, A. B., Fenwa, O. D., Oguntoye, J. P., Olayiwola, D. S., & Adeleke, A. J. (2025). Comparative analysis of score level fusion techniques in multi-biometric system. *LAUTECH Journal of Engineering and Technology*, *19*(1), 128-141.

Atanda, O. G., Ismaila, W., Afolabi, A. O., Awodoye, O. A., Falohun, A. S., & Oguntoye, J. P. (2023, April). Statistical Analysis of a deep learning based trimodal biometric system using paired sampling T-Test. In *2023 International Conference on Science, Engineering and Business for Sustainable Development Goals (SEB-SDG)* (Vol. 1, pp. 1-10). IEEE.

Ayangbekun O.J., Oladosu J.B., Ipeayeda F.W., Makinde O.E., Falohun A.S., Awodoye O.O., and Ige O.B. (2026). Benchmarking Modified Cheetah Optimization for Image Recognition Against Chicken and Chameleon Swarm Models. FUOYE Journal of Engineering and Technology (FUOYEJET), 11(1), 104-108.

Iranmanesh, V., Ahmad, S. M. S., Adnan, W. A. W., Yussof, S., Arigbabu, O. A., & Malallah, F. L. (2014). Online handwritten signature verification using neural network classifier based on principal component analysis. *The Scientific World Journal*, *2014*(1), 381469.

Kao, H. H., & Wen, C. Y. (2020). An offline signature verification and forgery detection method based on a single known sample and an explainable deep learning approach. *Applied Sciences*, 10(11), 3716.

Ogundepo, O. Y., Omeiza, I. O. A., & Oguntoye, J. P. (2022). Optimized textural features for mass classification in digital mammography using a weighted average gravitational search algorithm. *International Journal of Electrical and Computer Engineering (IJECE)*, *12*(5), 1-12.

Oguntoye, J. P., Ajagbe, S. A., Adedeji, O. T., Awodoye, O. O., Adetunji, A. B., Omidiora, E. O., & Adigun, M. O. (2025). An Improved Chicken Swarm Optimization Techniques Based on Cultural Algorithm Operators for Biometric Access Control. *Computers, Materials & Continua*, *84*(3).

Oguntoye, J. P., Awodoye, O. O., Oladunjoye, J. A., Faluyi, B. I., Ajagbe, S. A., & Omidiora, E. O. (2023). Predicting COVID-19 from chest X-ray images using optimized convolution neural network. *LAUTECH Journal of Engineering and Technology*, *17*(2), 28-39.

Sathya, R., Ananthi, S., Rupika, R., Santhiya, N., & Lavanya, K. (2022). Average Intensity Sign (AIS) Feature based Offline Signature Verification for Forgery Detection using Machine Learning. *International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, 2022(24), 325-330.

Sharif, M., Khan, M. A., Faisal, M., Yasmin, M., & Fernandes, S. L. (2020). A framework for offline signature verification system: Best features selection approach. *Pattern Recognition Letters*, 139 (2020), 50-59.

Sharma, N., Gupta, S., & Mehta, P. (2021). A comprehensive study on offline signature verification. *Journal of Physics: Conference series*, 1969(1), 012044.

Shrivastava, R., Shrivash, B. K., & Mandhan, N. (2016). Offline signature verification using SVM method and DWT-Gabor filter feature extraction. *Int J Sci Technol Eng*, 2(7), 232-237.

Summra, S., Usman, M. G., and Muhammad, A. (2021). Supervised Neural Network for Offline Forgery Detection of Handwritten Signature. *18th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE)*, IEEE (2021), 1-6.

Xuxin, C., Ximin Wang, K., Kar-Ming F., Theresa C. Thai, K. M., Robert S. M., Hong L., Bin Z., & Yuchen Q. (2022). Recent advances and clinical applications of deep learning in medical image analysis. *Medical Image Analysis*, 79 (2022), 102444.