Development of an Improved Signature Identification and Validation System using Cheetah Optimization Algorithm

[1]Ayangbekun O. J., [2]Oladosu J. B. and [3]Falohun A. S.

[1,2,3]Department of Computer Engineering, Faculty of Engineering and Technology, Ladoke Akintola University of Technology, Ogbomoso, Nigeria.

https://www.laujet.com/

ABSTRACT

Signature is a behavioral biometric characteristic popularly used for identity verification and validation to ensure the integrity and reliability of signed documents. The Convolutional Neural Network (CNN) model has been applied to several image-processing tasks involving image recognition and classification systems. Meanwhile, the major problems associated with the CNN approach include overfitting, parameter sensitivity and inefficient convergence as much time is spent on the solution space; with respect to inter-class variability. This research optimizes CNN hyperparameters using Cheetah Optimizer (CO), one of the most recent optimization techniques with standard benchmark functions in terms of performance for learning images; to differentiate a genuine signature from a forged signature. The system was trained on a large dataset of 5,220 handwritten signatures, incorporating into the model an advanced network architecture utilizing state-of-the-art algorithms to enhance its performance. 70% of the images were allocated as training datasets, 20% for testing and 10% for validation using the Random Sampling Cross Validation (RSCV) method. Evaluation methodologies were carried out on both CNN and CO-CNN models with MATLAB R2023a using confusion matrix metrics parameters to detect and distinguish between genuine and forged signatures, and its potential adoption in fraud detection and prevention. Results obtained demonstrate that Cheetah Optimized CNN (CO-CNN) outperforms the standard CNN in terms of accuracy and efficiency. CO-CNN achieved a higher Accuracy of 97.03% compared to 95.84% with CNN and; lower False Positive Rate (FPR) of 2.76% versus 3.89% for CNN. Precision, Sensitivity, and Specificity were also improved in CO-CNN, indicating better overall classification performance. Additionally, CO-CNN significantly reduced the computation time to 168.27 seconds, compared to 211.12 seconds for CNN, further validating its efficiency.

Keywords:

CNN,
CO-CNN,
Forged,
Genuine, Metrics,
Signature.

Corresponding Author:
ayangbekunoj@gmail.com:
+2348066380934

INTRODUCTION

Background of Study

Signature verification is of paramount importance in ensuring the integrity and reliability of signed documents, preventing fraud and ensuring legal validity. This makes signature verification a critical process that ensures the authenticity and integrity of documents, transactions, and identities. Handwritten signatures have been used as a widely accepted method of personal authentication and authorization for legal, financial, and administrative purposes for centuries (Hafemann *et al.,* 2017).

With the growing digital world, there is an increasing need for accurate and reliable signature recognition systems to prevent fraud and ensure security. Handwritten signature forgery is a significant concern, and traditional signature recognition methods may not be effective in detecting sophisticated forgeries. Developing more advanced and robust techniques is crucial to stay ahead of forgers who continuously improve their techniques.

Deep learning has shown remarkable success in various computer vision tasks, including image recognition and object detection. Conventional approaches for signature verification and forgery detection had problems of authenticity and consistency as they heavily relied on human judgment. The manual technique of verification and detection required a lot of time and is prone to individual biases or discrepancies (human error). Additionally, the quality of the signatures that were collected hindered their capacity to be reliable in real-world settings (Hafemann *et al.,* 2017). Applying deep learning to the problem of signature recognition can lead to significant improvements in accuracy and forgery detection capabilities. The use of the Cheetah Optimization Algorithm will introduce a novel aspect to the study. This optimization technique might offer an advantage over other optimization algorithms by potentially speeding up the convergence and improving the overall performance of the deep learning network model.

Current signature verification and forgery detection systems, which often depend on deep learning techniques like Convolutional Neural Networks (CNN), present another challenge. These techniques are computationally costly and inappropriate for real-time applications because they need intensive data preparation and hyperparameter adjustment (Bhatt *et al.,* 2021). Additionally, certain machine learning techniques, such as CNN, are vulnerable to problems like overfitting, which limit accuracy and generalization ability (Alajrami *et al.,* 2020; Espinosa-Leal *et al.,* 2021; Oguntoye *et al.,* 2023). Therefore, a novel strategy is required to address these problems and improve the accuracy and reliability of systems for handwritten signature authentication and forgery verification. However, finding the ideal balance between exploration and exploitation search strategies is the main issue, coupled with inefficient convergence which is hampered if the algorithm spends too much time examining unproductive regions of the solution space thereby leading to prematurely converging to a local optimum; missing out on potentially better solutions that are available in other parts of the search space (Akbari *et al.,* 2022). It is worthy of note that there is no one-size-fits-all network that performs optimally for all problems.

The architecture of a CNN is determined by its hyper parameters' values and plays a crucial role in its performance if well-tailored. Hence to tackle hyperparameter issues effectively, Cheetah Optimizer (CO) as one of the metaheuristics optimization algorithms are highly efficient (Bacanin *et al.,* 2021) as an approximate technique designed to find solutions that may not be the absolute best but are close to the optimal outcome. Cheetah optimizer is a type of optimization algorithm inspired by the hunting behaviour of cheetahs, which are known for their incredible speed and agility. It is a population-based nature–inspired stochastic search optimization algorithm method mimicking the behaviour of cheetahs in pursuit of their prey. The strengths of the Cheetah Algorithm lie in its fast or rapid convergence nature, especially in the early stages of search, and its effective global optimization features to be able to find global optima even in complex and multimodal landscapes. It is regularly employed in computational intelligence and complex optimization problems. However, inadequate parameter tuning can significantly impact the algorithm's convergence speed and quality of solutions (Akbari *et al.,* 2022; Atanda *et al.,* 2023). Meanwhile, the weakness of the Cheetah Algorithm includes: its heavy dependence on parameter settings (e.g., learning rate, population size); getting stuck (tapping) in local optima, especially in highly multimodal landscapes (due to poor parameters tuning); and its computationally expensive as it requires significant computational resources, particularly for large populations. However, CO still provides solutions to problems associated with the CNN technique much more efficiently. Meanwhile, the Cheetah Optimization (CO) algorithm can still be modified (MCO-CNN) for best performance and optimal solution.

LITERATURE REVIEW

Biometric Features

Identification of human beings is generally fundamental in everyday life, daily activities which are not limited to but include crossing international boundaries, gaining entrance to secure areas and traditional bank checks (Suman and Kumar, 2020; Oguntoye *et al.,* 2025a). Biometric verification helps to identify individuals based on their prominent physical or behavioural features (Ige *et al.,* 2025; Oguntoye *et al.,* 2025b).

The physiological biometric static features are unique physical characteristics that can be used to identify and verify an individual's identity (Adetunji *et al.,* 2018; Akintunde *et al.,* 2025). This type of biometric includes face, fingerprint, ear, palm print, retina, hand, finger geometry and DNA (Alsaadi, 2021; Yang *et al.,* 2021). The behavioural biometric features on the other hand include features that measure the person's actions, such as speaking, body motion, signature and writing (Alsaadi, 2021; Yang *et al.,* 2021). These features are not static because they change over time due to age effects and other developmental and enhancement factors.

Variability of Signatures

Signature, a behavioural biometric feature is a very important popular biometric trait (Lai and Jin, 2018). There are three fundamental areas of signatures in terms of establishing their authenticity and validation. The signature can be genuine, forged, and disguised. It should be noted that signatures can only be successfully verified if the intra-personal differences are less than the interpersonal differences (Nguyen et al., 2008).

A genuine signature is a signature which the real author creates under a normal condition whereby the author isn't limited by any guidelines. Few variables such as age, time, propensities, psychological or mental state, physical and practical conditions influence the signature of each individual (Hamadene *et al.,* 2023). On the other hand, Forged signatures are the handwriting of an impostor with the main aim of being perceived as genuine signatures of another person. The personal composing attributes of the forgers can even be evident and observed in their forgeries (Gonzalez-Garcia *et al.,* 2023). Be that as it may, the forgers can become increasingly skilled through training and critical improvement is often noticed when the forger is spurred (Mosaher and Hasan, 2022).

The forger is aware of the form of the original and has the necessary training to imitate it (Gosai *et al.,* 2022). Meanwhile, Disguised Signature is the kind of signature that is intentionally altered or modified to conceal the Signer's identity. It may be used to avoid detection or to create a new identity. Disguised signatures are those created when a bona fide signatory makes the signatures to dismiss the signed documents' genuineness later (Huang and Lu, 2023). These signatures are authored by valid clients and take after genuine ones; however, they contain features frequently found in forged signatures.

Cheetah Optimizer

Cheetahs are swift creatures with distinctive spotted coats, rapid returns during predation, and covert movement. They are limited in their ability to sustain speed; thus, they carefully scan the area while perched on tiny trees or slopes to see their prey. Cheetahs sit in one spot after seeing the prey, watch until it approaches, and then launch an assault. There are stages of rushing and capturing prey in the assault mode: Exploration; Patience and Waiting; Attack; Withdraw and go back home (Akbari *et al.,* 2022).

METHODOLOGY

Research Approach

Developing a Cheetah Optimizer Convolutional Neural Network (CO-CNN) for a handwritten-signature identification system for the best performance and evaluation involves the following stages (Fig. 1): Data acquisition stage; which involves obtaining handwritten signature images from a pool of five thousand, two hundred and twenty images (5220) with 10 samples of signatures per individual for two hundred and seventy-five (275) genuine and two hundred and forty-seven (247) forged signatures. Datasets are analytically allocated 70% for training, 20% for testing and 10% for validation using the random sampling cross-validation method. The next stage is to pre-process and segment the acquired data images as shown in Figure 2. Pre-processing techniques involve conversion to grayscale, noise reduction, image normalization and thinning with skew.

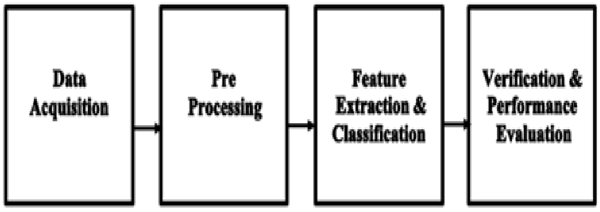

Figure 1: Research Framework

Development of Handwritten-signature Recognition System using CO-CNN

The primary focus of this system is to establish a method for categorizing handwritten signature images through the utilization of deep learning Convolutional Neural Networks (CNNs). The images of handwritten signatures are differentiated into genuine and forged categories. Input to the system comprises these images, and the output is the accurately classified image. The CNN is optimized by incorporating the Cheetah Optimizer (CO) algorithm. This optimization technique involves retraining the CNN with handwritten signature images to achieve precise classification outcomes. This proposed approach effectively enhances the CNN network's efficiency through the utilization of pre-trained CNN networks, specifically RESNET. To attain optimal performance, hyper-parameters like the learning rate and filter size of the CNN are fine-tuned using the CO algorithm. This is because if the learning rate is high the network may converge too quickly but if the learning rate is too low it may lead the network to lose important details in the data (Oguntoye *et al.,* 2023; Olayiwola *et al.,* 2023).

The optimization of Hyper-parameter

This study employs the CO algorithm within the classifier section of CNN architecture models to optimize the batch size and dropout layer rate. The overall methodology is illustrated in Figure 3, depicting the flowchart of the Convolutional Neural Network with Cheetah Optimizer (CO-CNN). The training process operates in an iterative loop, concluding when all cheetahs generated by the CO have been assessed for each generation. The steps for optimizing the CNN using the CO algorithm are depicted in Figure 3 and elucidated using the following steps:

i. provide handwritten signature database for CNN training

ii. generate cheetah population for CO algorithm.

iii. initialize CNN architecture.

iv. CNN training and validation.

v. Evaluate the objective function to determine the best value.

vi. Update CO parameters.

vii. Repeat the process and evaluate the cheetahs until the stop criteria are found (the number of iterations).

viii. Select the optimal CNN parameters.

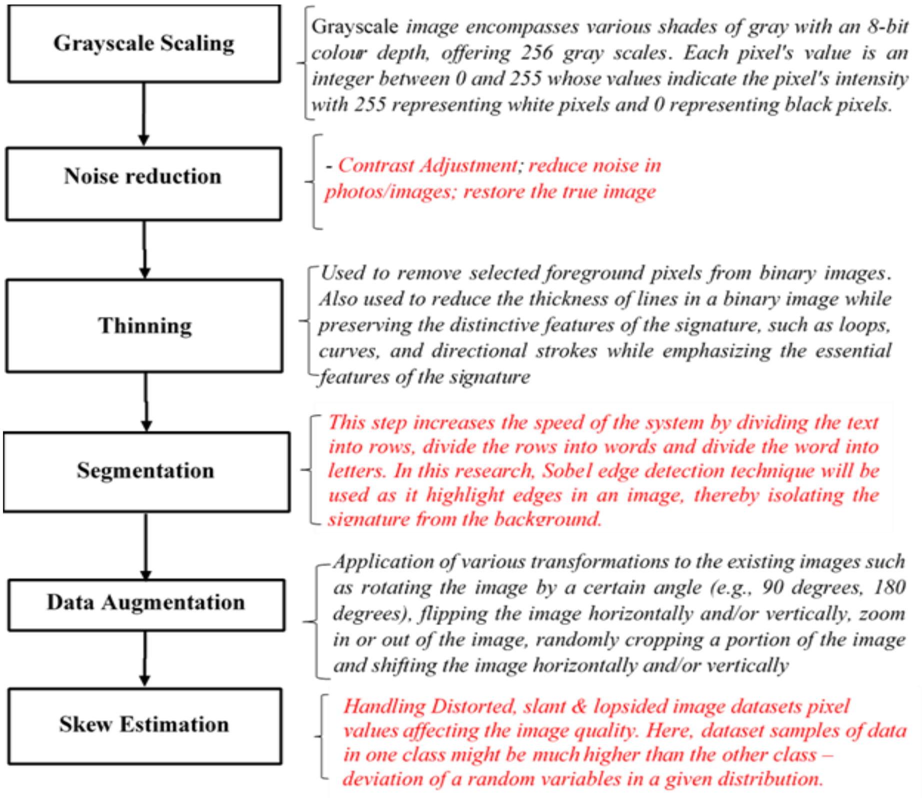

Figure 2. Data Pre-processing stages

Implementation of CO-CNN for the Handwritten-signature Recognition

A user-friendly Graphic User Interface (GUI) application will be created, incorporating a local database containing digit images of handwritten signatures. The GUI design leverages toolboxes such as image processing, deep learning, and optimization within MATLAB 2023a environment. Then the implementation is carried out using the MATLAB software package on a computer system with a defined configuration.

Evaluation Measures

The evaluation of the CO-CNN technique in the handwritten signature recognition system in this paper is based on confusion matrix performance metrics: False Positive Rate, Precision, Sensitivity, Specificity, Accuracy, and computation Time. The correctly identified foregrounds are termed true positives (TP), while undetected foregrounds are referred to as false negatives (FN). Objects falsely identified are labelled as false positives (FP), and true negatives (TN) denote objects not incorrectly identified as background.

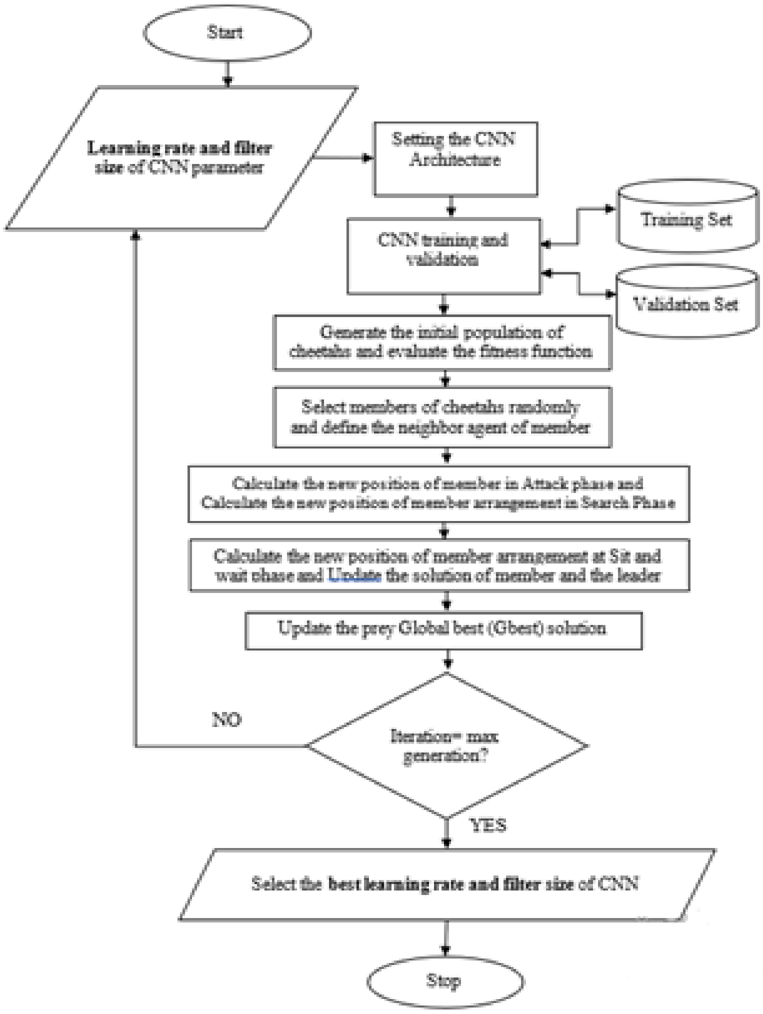

Figure 3: Flow diagram of Convolutional Neural Network with Cheetah Optimizer (CO -CNN)

RESULTS AND DISCUSSION

The results of the evaluation of the signature identification system using the Convolutional Neural Network (CNN) approach and Cheetah Optimized Convolutional Neural Network (CO-CNN). The pre-processed and segmented images used for the study were grouped into genuine and forged; for the training and testing phase (Fig. 4). The performance metrics were analysed using a square dimension pixel resolution at different average thresholds of 0.25, 0.35, 0.45 and 0.75 from a range of threshold of 0-0.25, 0.26-0.35, 0.36-0.45 and 0.46-0.75 respectively. The dataset used in this study consists of two thousand four hundred and seventy (2470) forged signatures and two thousand seven hundred and fifty (2750) genuine signatures; out of which 10 samples of signature images per two hundred and seventy-five (275) genuine and two hundred and forty-seven (247) forged individuals' signature were collected.

The evaluation of the results of the technique was based on False Positive Rate (FPR), Precision, Sensitivity, Specificity, Accuracy and Recognition/Computation Time for each of genuine and forged datasets as shown in Table 1 for both CNN and CO-CNN. However, the optimum threshold for both techniques was achieved at a 0.75 threshold value.

Table 1: Automated Classified Forged and Genuine Signatures

	Categories	CNN	CO-CNN	Total
FORGED	Correctly Forged (TP)	2360	2391	4751
	Misclassified as Genuine (FN)	110	79	189
	TOTAL (Forged)	2470	2470	4940
GENUINE	Correctly Genuine (TN)	2643	2674	5317
	Misclassified as Forged (FP)	107	76	183
	TOTAL (Genuine)	2750	2750	5500

Results Evaluation for CNN

For the CNN technique at an optimum threshold of 0.75, the forged dataset which is made up of 2470 forged signature image datasets, 2360 datasets were classified correctly as forged, 110 signature image datasets were misclassified as genuine while out of 2750 genuine signature image datasets, 2643 signature image datasets were classified correctly as genuine and 107 signature image datasets were misclassified as forged (Table 1).

The results obtainable at an optimum threshold value of 0.75 discloses that CNN on the signature dataset had an average FPR of 3.89 %, Precision of 95.66%, Sensitivity of 95.55%, Specificity of 96.11%, and Accuracy of 95.84% at 211.12 seconds.

Figure 4: Training / Testing Phase GUI

Results Evaluation for CO-CNN

Table 1 demonstrates the results achieved through CNN and the application of the Chetah Optimizer to CNN (CO-CNN) technique, specifically at various thresholds. Out of 2470 forged signature image datasets, 2391 were accurately identified as forged, while 79 were mistakenly classified as genuine. Likewise, out of 2750 genuine datasets, 2674 were correctly identified as genuine, with 76 being misclassified as forged (Table 1). At the optimal threshold of 0.75, the CO-CNN approach yielded an average False Positive Rate (FPR) of 2.76%, Precision of 96.92%, Sensitivity of 96.80%, Specificity of 97.24%, and Accuracy of 97.03%, all achieved within 168.27 seconds.

Comparison Results among CNN and CO-CNN

Table 2 below shows the combined results of CNN and CO-CNN in identifying signature datasets for all metrics; at 0.75 optimum threshold value. It indicates CO-CNN technique has a lower recognition time compared with the corresponding CNN technique. Similarly, FPR, sensitivity, specificity, accuracy and recognition time of CO-CNN and CNN techniques were compared; the study discovered that the CO-CNN technique has better performance in accuracy, sensitivity, specificity, precision, and false positive rate than the CNN technique as enumerated in Table 2. CNN technique produces FPR at 3.89 %, Precision at 95.66%, Sensitivity at 95.55%, Specificity at 96.11%, and recognition accuracy of 95.84% at 211.12 seconds. CO-CNN technique on the other hand generated a False Positive Rate (FPR) of 2.76%, Precision of 96.92%, Sensitivity of 96.80%, Specificity of 97.24%, and Accuracy of 97.03%, all achieved within 168.27 seconds. The graphical illustration of both techniques is represented in Figure 5.

Table 2: Summary of Performance Evaluation of CNN and CO-CNN at the Optimal Threshold

Algorithm	FPR	Precision (%)	Sensitivity (%)	Specificity (%)	Accuracy (%)	Time (sec)
CNN	3.89	95.66	95.55	96.11	95.84	211.12
CO-CNN	2.76	96.92	96.80	97.24	97.03	168.27

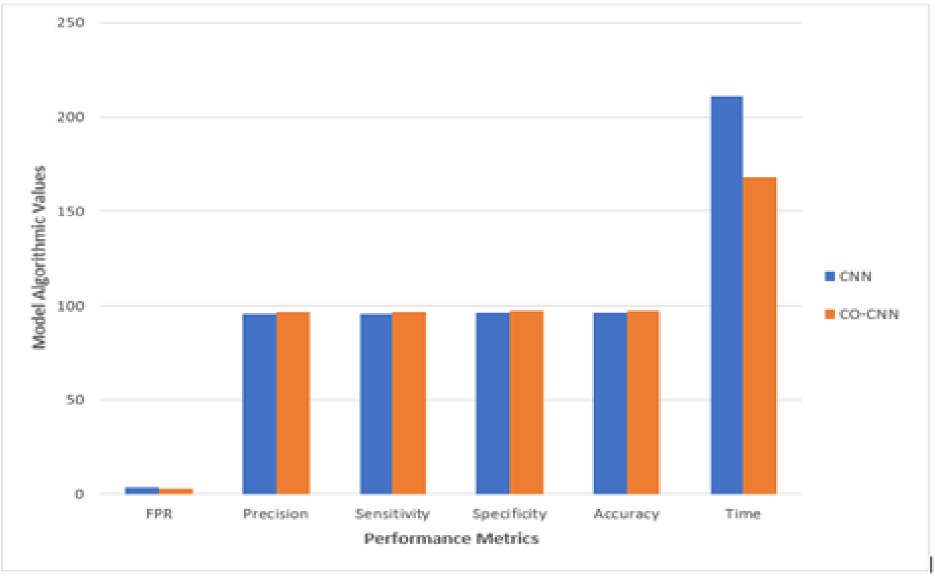

Figure 5: CNN and CO-CNN Optimal Threshold Performance Evaluation

Discussion of Results

The results evaluation described the performance of the classifier technique showing significant variation in the performance across all metrics indicators - FPR, precision sensitivity, specificity, and accuracy for both CNN and CO-CNN classification schemes respectively. Considering the comparative analysis of both techniques, the optimization of the CNN parameters by CO contributed immensely by improving the recognition percentage and reducing computational time. The CO-CNN technique has a lower false positive rate decrement of 1.13%, precision of 1.74%, sensitivity of 1.25%, an increment of specificity of 1.13%, and accuracy of 1.19% at a time interval of 42.85 seconds for Genuine and Forged datasets as optimum threshold compared with CO-CNN. The performance of CO-CNN was a result of optimal selection of its weight and learning rate by CO; as represented in Figure 5.

CONCLUSION

This research has contributed immensely to the body of knowledge by developing a new approach for handwritten signature verification and forgery detection using CNN based Cheetah Optimization (CO-CNN) technique. The Cheetah Optimizer selects some optimal CNN hyper-parameters learning rate and filter size to improve generally the recognition performance of handwritten signatures at reduced computation time. For future research work, CO-CNN can be modified (MCO-CNN) for better performance evaluation analysis and compared with that of the CO-CNN technique.

REFERENCES

Adetunji A. B., Oguntoye J. P., Fenwa O. D. and Akande N. O. (2018). Web Document Classification Using Naïve Bayes. Journal of Advances in Mathematics and Computer Science. 29(6): pp, 1-11.

Akbari, M. A., Zare, M., Azizipanah-Abarghooee, R., Mirjalili, S., and Deriche, M. (2022). The Cheetah Optimizer: A Nature-inspired Metaheuristic Algorithm for Large-scale Optimization Problems. *Scientific reports*, 12(1), 10953.

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.

Alajrami, E., Ashqar, B. A., Abu-Nasser, B. S., Khalil, A. J., Musleh, M. M., Barhoom, A. M. and Abu-Naser, S. S. (2020). Handwritten Signature Verification using Deep Learning. *International Journal of Academic Multidisciplinary Research (IJAMR),* 3(12): 39-44.

Alsaadi, I. M. (2021). Study on Most Popular Behavioural Biometrics, Advantages, Disadvantages and Recent Applications: *A review. Int. J. Sci. Technol. Res,* 10(1).

Atanda, O. G., Ismaila, W., Afolabi, A. O., Awodoye, O. A., Falohun, A. S., & Oguntoye, J. P. (2023). 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.

Bacanin, N., Stoean, C., Zivkovic, M., Jovanovic, D., Antonijevic, M., and Mladenovic, D. (2022). Multi-Swarm Algorithm for Extreme Learning Machine Optimization. *Sensors,* 22(11), 4204. https://doi.org/10.3390/s22114204

Bhatt, D., Patel, C., Talsania, H., Patel, J., Vaghela, R., Pandya, S., Modi, K. and Ghayvat, H. (2021). CNN Variants for Computer Vision: History, Architecture, Application, Challenges and Future Scope. *Electronics,* 10(20), p.2470.

Espinosa-Leal, L., Akusok, A., Lendasse, A., and Björk, K. M. (2021). Extreme Learning Machines for Signature Verification. In Proceedings of ELM2019 9. *Springer International Publishing.*

Gonzalez-Garcia, C., Tolosana, R., Vera-Rodriguez, R., Fierrez, J., and Ortega-Garcia, J. (2023). Introduction to Presentation Attacks in Signature Biometrics and Recent Advances. Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment, 447-466.

Gosai, D., Vyas, S., Patel, S., Barot, P. and Suthar, K. (2022). Handwritten Signature Verification Using Convolution Neural Network (CNN). *An International Conference on Advancements in Smart Computing and Information Security* (pp. 90-106). Cham: Springer Nature Switzerland.

Hafemann, L. G., Sabourin, R. and Oliveira, L. S. (2017). Offline Handwritten Signature Verification—literature Review. In 2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA). IEEE.

Hamadene, A., Ouahabi, A. and Hadid, A. (2023). Deep Fakes Signatures Detection in the Handcrafted Features Space. *In Proceedings of the IEEE/CVF International Conference on Computer Vision* (pp. 460-466).

Huang, F. H. and Lu, H. M. (2023). Multiscale Feature Learning using CO-tuplet Loss for Offline Handwritten Signature Verification. arXiv preprint arXiv:2308.00428.

Ige, O.B., Falohun, A.S., Omidiora, E.O., Olabiyisi, S.O., Ige, R.O., Oguntoye, J.P., Awodoye, O.O., Adedeji, O.T. and Oke, A.O. (2025). Development of an enhanced support vector machine face recognition system. LAUTECH Journal of Engineering and Technology, 19(2), 30-40.

Lai, S. and Jin, L. (2018). Recurrent Adaptation Networks for Online Signature Verification. IEEE *Transactions on Information Forensics and Security,* 14(6), 1624-1637.

Mosaher, Q. S. U. and Hasan, M. (2022). Offline Handwritten Signature Recognition using Deep Convolution Neural Network. *European Journal of Engineering and Technology Research,* 7(4), 44-47.

Nguyen, V., Blumenstein, M., Muthukkumarasamy, V. and Leedham, G. (2007). Off-line Signature Verification using Enhanced Modified Direction Features in Conjunction with Neural Classifiers and Support Vector Machines. *In Ninth International Conference on Document Analysis and Recognition* (ICDAR 2007). IEEE.

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.

Oguntoye, J. P., Ajagbe, S. A., Adedeji, O. T., Awodoye, O. O., Adetunji, A. B., Omidiora, E. O., & Adigun, M. O. (2025a). An improved chicken swarm optimization technique based on cultural algorithm operators for biometric access control. *CMC-Computers, Materials & Continua,* 1-20. https://doi.org/10.32604/cmc.2025.062440

Oguntoye, J. P., Adedeji, O. T., Alade, O. M., Olayiwola, A. A., Omidiora, E. O., & Adetunji, A. B. (2025b). Multi-instance iris biometric authentication system based on cultural chicken swarm optimization technique. *FUW Trends in Science & Technology Journal, 10*(1), 127–133.

Olayiwola, D. S., Olayiwola, A. A., Oguntoye, J. P., Awodoye, O. O., Ganiyu, R. A., & Omidiora, E. O. (2023). Development of a Fingerprint Verification and Identification System Using a Gravitational Search Algorithm-Optimized Deep Convolutional Neural Network. *Adeleke University Journal of Engineering and Technology*, *6*(2), 296-307.

Suman, R. and Kumar, D. (2020). Punjabi Offline Signature Verification System Using Neural Network.

Yang, W., Wang, S., Sahri, N. M., Karie, N. M., Ahmed, M. and Valli, C. (2021). Biometrics for Internet-of-Things Security: A review. *Sensors,* 21(18), 6163.