Improved Electric Eel Foraging Optimization-Based Convolutional Neural Network for Two-Level Captcha Authentication Using Facial Emotion Recognition

Adeyemi, Biliqees Temitope[1], Makinde, Oladayo Ezekiel[2], Ojo, Olufemi Samuel[3]

[1], Department of Computer Science, Kwara State College of Education, Ilorin, Nigeria
[2, 3] Department of Computer Science, Ajayi Crowther University, Oyo, Nigeria

ABSTRACT

This study describes an Improved Electric Eel Foraging Optimization-Based Convolutional Neural Network (IEEFO-CNN) for two-level CAPTCHA validation based on facial expression recognition. The traditional CAPTCHAs are no longer resistant to the attacks of artificial intelligence, so the need for a more secure CAPTCHA to certify the cognitive and behavioural fact that the user is indeed a human still exists. An Improved Electric Eel Foraging Optimization algorithm incorporating adaptive energy factor control, elite preservation, dynamic migration, and Levy flight exploration was developed to optimize CNN hyper parameters. To put the proposed method to the test, we carried out an experimental evaluation using a real-world data set of 2,000 facial images from 500 different subjects. The numbers speak for themselves: our new IEEFO-CNN is shown to be an effective way of bolstering authentication security on the web and social media. With reference to performance, it has an accuracy of 98.50 per cent and an AUC of 0.98. False Acceptance Rate of 0.33%, a False Rejection Rate of 2.67% and an Equal Error Rate of 1.50% were also recorded.

KEYWORDS

Authentication, Algorithm, Hyper parameters, Security, Optimization, Improved

I. INTRODUCTION

The growing development of internet and social media platforms requires user account authentication methods to become more secure as bots are now used to bypass authentication security. CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) is one of the methods used to differentiate between genuine users and bots (Guerar and Migliardi, 2022). Conventional CAPTCHA employs a layer system of text, image or challenge-response tests for spam, account creation, and access (Noury and Rezaei, 2020). However, with recorded breakthrough and progresses in artificial intelligence and deep learning, many CAPTCHA systems can be solved with high accuracy by machine teaching (Tariq et al., 2023).

According to Trong et al., (2023), the possibility of multiple-layer human authentication security system has attracted the interest of the Cyber security research community. A promising method of behavioural biometrics in facial emotion recognition is based on the fact that facial emotions are varied and non-replicable.

Deep learning based on Convolutional Neural Networks (CNNs) facilitates the automatic extraction of facial features, which results in improved facial emotion recognition (Khan et al., 2020). However, CNN performance depends on its hyper parameters. Optimization is very important in improving the accuracy of facial emotion recognition (Zhang et al., 2023; Ali et al., 2024). Although, the Electric Eel Foraging Optimization (EEFO) algorithm is a nature-inspired high-level algorithmic framework with commendable output during optimization, it is not free from errors (Wang et al., 2023; Zhao et al., 2024).

Accordingly, in this work, Improved Electric Eel Foraging Optimization-based Convolutional Neural Network (IEEFO-CNN) is presented to develop a two-level CAPTCHA authentication system for facial emotion recognition. Consequently, the conventional EEFO has been improved and adapted by applying adaptive migration, adaptive Levy flight, adaptive elite preservation, and adaptive energy control. The system combines CAPTCHA authentication with facial emotion recognition by using CNN for receiver operations and explaining its functionality and efficiency through accuracy, FAR, FRR, EER, AUC, and authentication time.

II. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

The developments in the cyber world has led to the invention of enhanced systems and applications, this has equally led to the evolution of cyber threats that has resulted in a variety of more advanced cyber security challenges. Among the challenges is the use of bots to bypass authentication systems. In order to address these challenges, scientists have developed advanced technologies such as CAPTCHA, emotion recognition, deep neural networks, and optimization methods. These technologies served as the basis for the proposed IEEFO-CNN authentication framework.

CAPTCHA is an obstacle-based system that restricts machine access by requiring users to solve tests, called CAPTCHA challenges that humans find easy but that machines find difficult. CAPTCHA challenges have been effective at preventing spam and automatic account generation. Nevertheless, new artificial intelligence and deep learning approaches have made it possible for machines to solve many CAPTCHA challenges, greatly reducing their ability to exclude machines. Emotion detection technology is an example of a behavioural biometric technology that has been developed to enhance authentication systems. In contrast to passwords and conventional biometrics, emotions involve user action and are difficult to copy or automate. Emotion recognition techniques identify emotional expressions, creating an extra verification component that improves resistance to spoofing and automated attacks.

Convolutional Neural Networks (CNNs) have been widely used in the field of facial image analysis because they can learn discriminative features automatically from images (Khan et al., 2020; Turay and Vladimirova, 2022). However, CNN-based facial image analysis requires hyper parameters for optimization and thus obtains better classification accuracy

and model efficiency. Electric Eel Foraging Optimization (EEFO), an optimization algorithm from the nature-inspired met heuristic family, has exhibited excellent search ability but still exhibits drawbacks such as premature convergence and decreased population diversity (Wang et al., 2023; Zhao et al., 2024). Prior works have mainly focused on the application of CAPTCHA, the facial emotion recognition, CNN, and optimization method in the field. This study addresses this gap by integrating these technologies within a unified framework using an Improved Electric Eel Foraging Optimization algorithm to enhance CNN-based two-level CAPTCHA authentication.

Table 1. Comparative Analysis of Existing Studies

Approach	**CAPTCHA**	**Recognition Of Emotion**	**Optimisation of CNN**	**Two-Level Authentication**
Orthodox CAPTCHA	Yes	No	No	No
Facial Identification Systems	No	Yes	No	No
CNN-Based Emotion Recognition	No	Yes	Yes	No
EEFO-CNN Models	No	Yes	Yes	No
Proposed IEEFO-CNN	Yes	Yes	Yes	Yes

III. MATERIALS AND METHODS

A. Research Framework

An experimental study is conducted to improve the multi-level CAPTCHA's using the facial emotion recognition in behavioural biometric authentication by presenting an Improved Electric Eel Foraging Optimization-Based Convolutional Neural Network (IEEFO-CNN) for the facial emotion recognition. The system proposed in this work consists of two main stages of a novel and two-step authentication flow. In the first stage of the system, in order to verify whether the user who is trying to log into a system is a human or automated bot, a text-based CAPTCHA is given to the user to be recognized by the system.

If recognized correctly by the system, in the second stage of the system, a facial emotion is captured by camera of camera-enabled device of the user is pre-processed by the Improved Electric Eel Foraging Optimization-Based Convolutional Neural Network (IEEFO-CNN) and the user is authenticated by the system only if both the CAPTCHA and facial emotion are recognised correctly by the system.

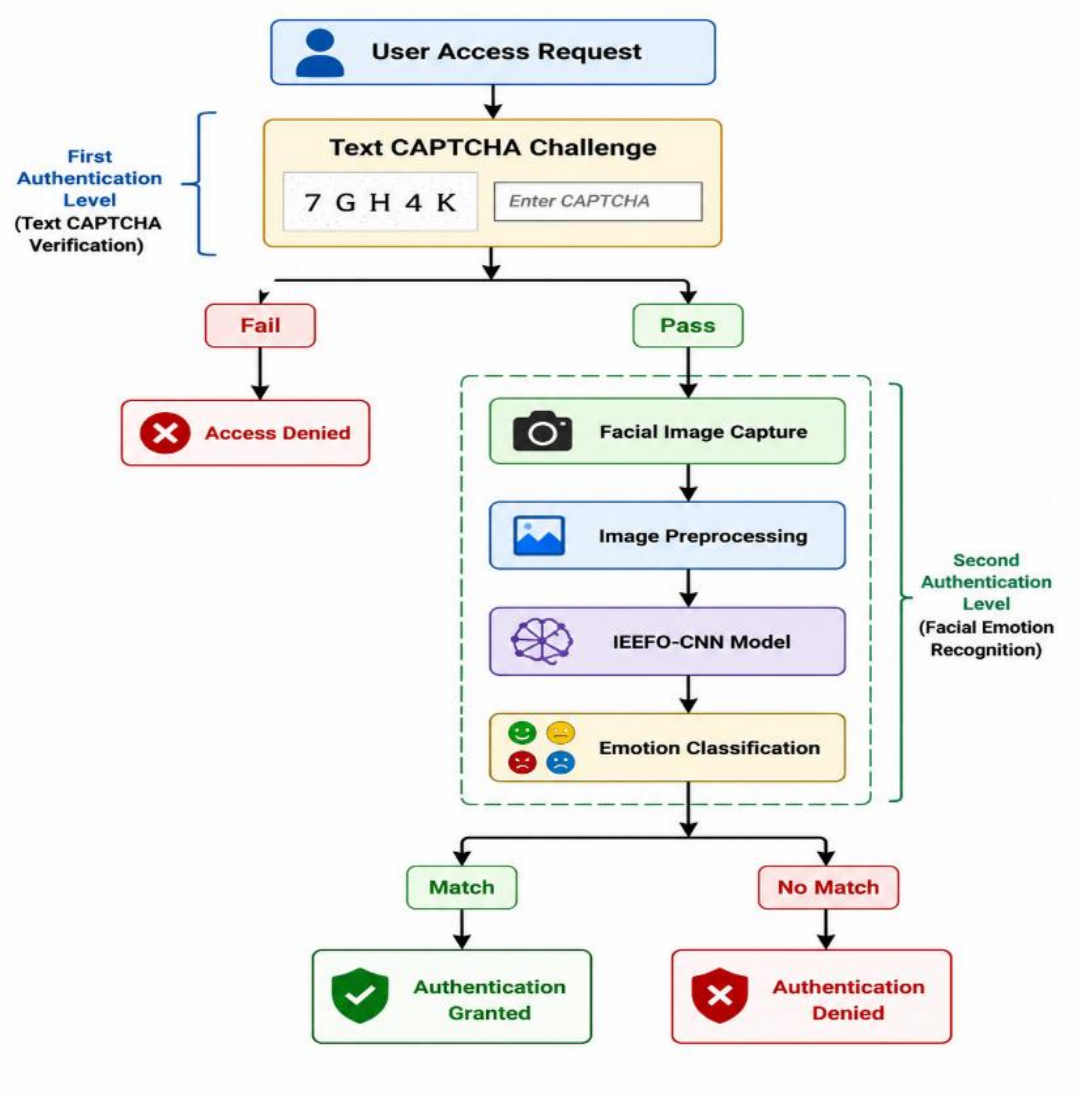

Figure 1: Proposed Two-Level CAPTCHA Authentication Framework

B. Dataset Description and Pre-processing

The dataset that is used for facial expressions recognition contains 2,000 grayscale images of 500 different faces. This research used four different expressions which are angry, happy, and sad and surprise as presented almost by the same number of samples, so the dataset is balanced. The dataset was divided to test set and train set in the ratio 30:70, so there are 1,400 images in the train set and 600 in the test set. All images used in the dataset were of high quality and after they were uploaded into system, they were normalised to size of 64x64 pixels and cleaned from noise to avoid interference. Also, there are several data-assisted operations carried-out on the images, like rotation and flipping of images.

Images go through normalization of pixel value normalization in order to enable fast learning as well as of resizing to appropriate size and noise reduction in order to get the best quality images and thus to get the best possible results. Besides, those images go through data augmentation (e.g. rotation). This increases diversity of already existing images in the given dataset and also the given model gets better generalization ability.

C. Convolutional Neural Network Architecture

For Facial- Emotion-based authentication, a Convolutional Neural Network (CNN) is implemented in the proposed system. The network starts from the input layer where the greyscale facial images are input to the system and then the images are processed through the layers of convolution, ReLu activators and pooling to detect edges, textures, etc. to extract the information of facial expression. The dimensions of the features are reduced in the pooling layers and the computation is reduced. The dropout layers are also added in the network to prevent over fitting of the network and to improve the generalization of the network. The network is followed by the fully connected layers and the Softmax output layer where each input image is classified into the four emotion categories.

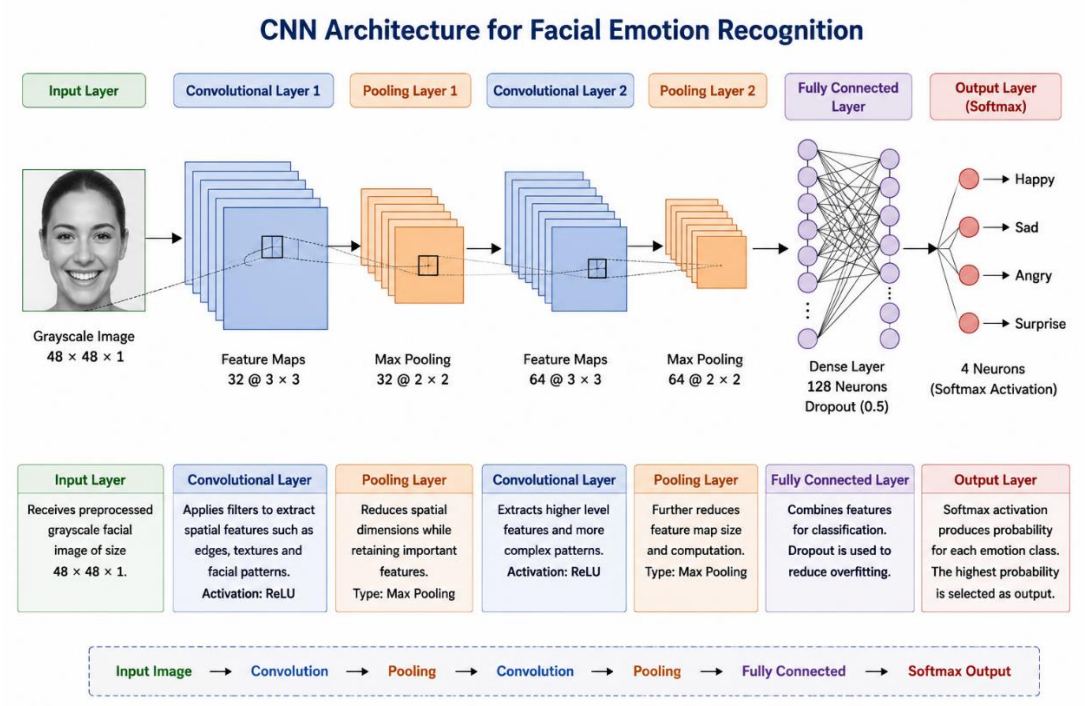

Figure 2: Facial Emotion Recognition CNN Framework

D. Improved Electric Eel Foraging Optimization Algorithm

Improved Electric Eel Foraging Optimization (IEEFO) for Hyper-parameters of CNN.

Electric Eel Foraging Optimization (EEFO) is a newly introduced algorithm inspired by the predatory skills, foraging activities and social behaviour of Electric Eels. EEFO has been applied and showed its effectiveness to several optimization problems. However, there are some drawbacks for this algorithm. It often converges to a local optimum early in the search process and there is a limited amount of variation in the population. Thus, a modification of the algorithm is proposed in this paper based on the enhancement of four approaches.

Improved Electric Eel Foraging Optimization (IEEFO) is an improved algorithm for optimizing the hyper parameters of a CNN, which is based on the modification of four approaches.
Adaptive Energy Factor Control.

The search space is to be explored more effectively in the early stages of search, and in subsequent stages the found possible solutions are to be fine-tuned in order to improve them and to achieve a faster convergence. Adaptive Energy Factor Control of the exploration / exploitation factor thus enhances the search space exploration.
Elite Preservation Strategy.

Elite Preservation Strategy: This strategy tries to preserve the best solutions found so far by copying them to the next generation. Thus, good solutions are not lost and the search process becomes more stable.

Dynamic Migration Mechanism: The search space of the Electric Eel Foraging Optimization (EEFO) algorithm is improved by global search. The candidate solutions that are found during the search in the solution space are transferred periodically to a shared solution pool. The solution pool changes during the search. So a global minimum is prevented from being found by the algorithm, which is stuck in a local minimum.

Levy Flight-Assisted Exploration: By using the jumps of the long size done by the Electric Eels (using the so-called Levy flights) to search for the optimal solution within the search space, the searches are scaled out of local minima and, thus, an effective exploration of the search space is carried out. The search quality and time cost of the EEFO are improved by the four enhancements for the EEFO to perform better.

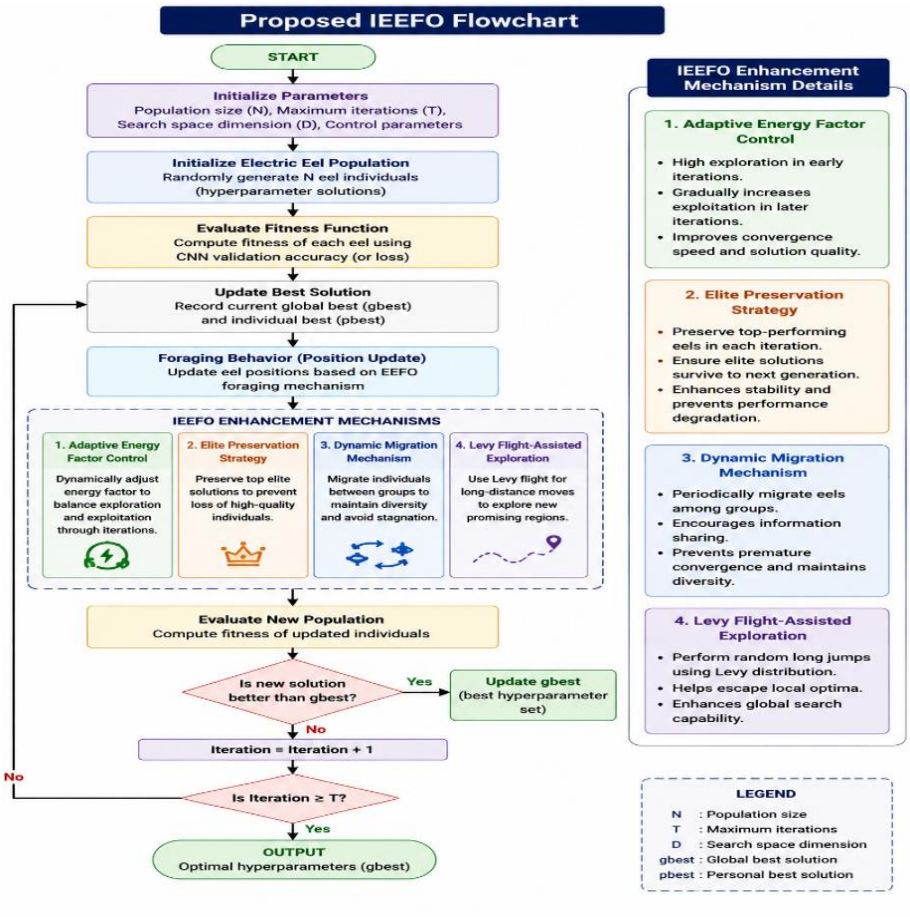

Figure 3: Proposed IEEFO Flowchart

E. Authentication Procedure

- A user attempts to access the protected system.
- The user is then tested by a text-based CAPTCHA if he succeeded in the first verification step.
- The user is requested to display a specific facial emotion, and the captured facial images of the user are processed by the IEEFO-CNN model. The predicted emotion of the user by the model is then compared with the emotion required for authentication.
- When the system recognizes the facial expression of the user it can determine if it matches the required expression to grant access. If the user's expression does not match, then access to the system will be denied

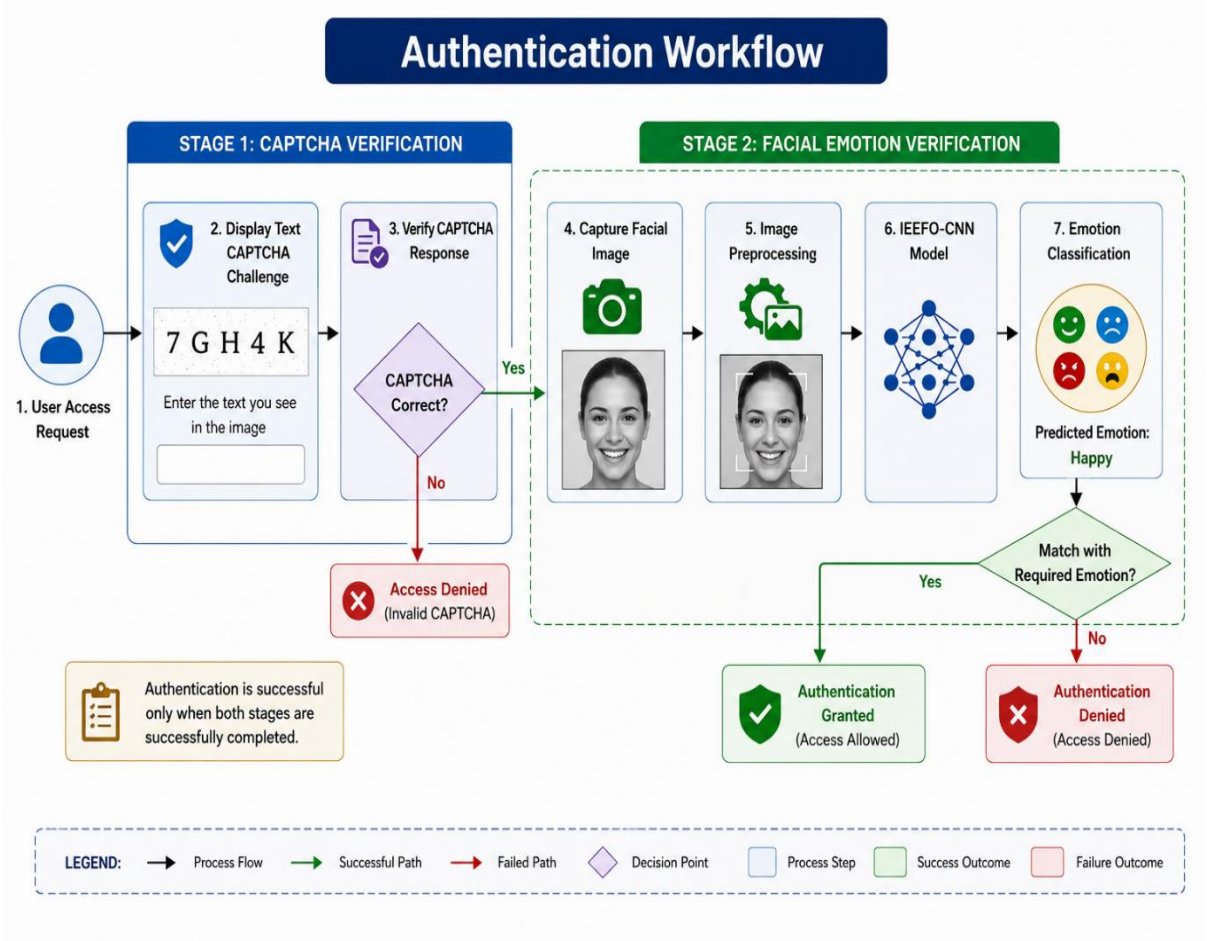

Figure 4: Authentication Workflow

F. Performance Evaluation Metrics

The performance of the proposed framework was evaluated by the commonly used classification and authentication performance measurements.

The effectiveness of the proposed framework was evaluated using standard authentication and classification performance metrics.

1. *Accuracy:* Accuracy is a performance measure and indicates how accurate a model is for classification. It calculates how many correct predictions a model has compared to the total number of failures. The equation for accuracy is given as follows:

   Accuracy = (TP+TN) / (TP+TN+FP+FN) x 100
   Where TP = True positive, TN = True negative, FP = False positive and FN = False negative

2. *False Acceptance Rate (FAR):* The False Acceptance Rate (FAR) is the ratio of the number of false accepted impostor claims, the equation for which is: FAR= (FP \FP+TN) ×100

3. *False Rejection Rate (FRR):* False Rejection Rate (FRR) The False Rejection Rate or (FRR) is the percentage of the true users that the system incorrectly rejects. It can be calculated with the use of this equation: FRR= (FN\TP+FN) ×100

4. *Equal Error Rate (EER):* Equal Error Rate (EER) is the threshold value where False Acceptance Rate (FAR) is equal to False Rejection Rate (FRR). It can be mathematically expressed as FAR (t) = FRR (t). In where, t is a decision threshold for a system for authentication. A low EER value indicates good authentication capability of a system. The area under the curve (AUC).

5. *Area under the Curve (AUC):* The Area under the Curve (AUC) is a statistical tool which can be used to compute the total area of the Receiver Operating Characteristic (ROC) curve of a classification system. A ROC curve is generated by a classification system and plots the True Positive Rate (TPR) of a classification system against the False Positive Rate (FPR) for different threshold levels. This is one of the most common measures to evaluate the capacity of a classification system to correctly classify into two different classes. Its score ranges from 0 to 1 where 1 is the highest possible score indicating that the system is optimal for classifying between the two classes.

   AUC = ∫0 TPR (FPR) d (FPR)
   Where: True Positive Rate (TPR): TPR = TP / (TP + FN) FPR = FP / (FP + TN)

G. Computational Complexity Analysis

The original EEFO algorithm has a complexity of O (TND) where T is the number of iterations, N is population size, and D is the number of decision variables. The complexity is expressed as: O (N.D.T) Although the IEEFO adaptively controls the energy, preserves the elite, migrates dynamically, and searches for new regions in the solution space with Levy flights, the proposed optimization method does not change the asymptotic computational complexity of EEFO. Thus, IEEFO achieves the same theoretical complexity as its ancestor method with better convergence properties and better solutions.

IV. RESULTS AND DISCUSSION

A. Overview of Experimental Results

The proposed Improved Electric Eel Foraging Optimised Convolutional Neural Network (IEEFO-CNN) framework was tested using a dataset of 600 facial emotion examples and then compared to a traditional Convolutional Neural Network (CNN) and an Electric Eel Foraging Optimised Convolutional Neural Network (EEFO-CNN). The comparative study was designed to assess the capability of the IEEFO-CNN framework's optimisation innovations on facial emotion recognition and authentication efficiency in the two-tier CAPTCHA mechanism.

B. Confusion Matrix Analysis

When used in the field of systems, confusion matrices are used to evaluate how well the classified samples are compared to the actual samples. This helps provide a good understanding of its characteristics. Confusion matrices being used in authentication systems give more insight on the acceptances and rejections of the system, and not only overall percentage of accuracy.

C. CNN Performance

Table 2. Confusion Matrix of CNN Model

Actual Class	**Predicted Genuine**	**Predicted Impostor**
Genuine User	233	67
Impostor	8	292

The CNN correctly identified 233 legitimate users and rejected 292 impostors. However, it incorrectly rejected 67 genuine users and falsely accepted 8 impostors. Although the CNN has reasonable classification ability, it has problems when dealing with variations in facial expressions.

EEFO-CNN Performance

Table 3. Confusion Matrix of EEFO-CNN Model

Actual Class	**Predicted Genuine**	**Predicted Impostor**
Genuine User	280	20
Impostor	5	295

Optimisation using EEFO significantly improved classification performance. Correct authentication decisions increased substantially, while both false acceptance and false rejection errors decreased. This improvement demonstrates the effectiveness of optimisation-driven hyper parameter selection in enhancing CNN learning capability.

IEEFO-CNN Performance

Table 4. Confusion Matrix of IEEFO-CNN Model

Actual Class	Predicted Genuine	Predicted Impostor
Genuine User	292	8
Impostor	1	299

The proposed IEEFO-CNN model attained the most favourable classification outcome amongst all evaluated architectures, correctly authenticating 292 genuine users whilst accurately rejecting 299 impostors. Across the entirety of the testing dataset, only nine classification errors were recorded, a result that substantively affirms the efficacy of the enhanced optimisation strategy in refining decision boundaries and minimising misclassification.

D. Comparative Authentication Performance

Table 5. Comparative Performance of Authentication Models

METRIC	CNN	EEFO-CNN	IEEFO-CNN
Accuracy (%)	87.50	95.83	98.50
FAR (%)	2.67	1.67	0.33
FRR (%)	22.33	6.67	2.67
EER (%)	13.20	6.83	1.50
AUC (%)	0.89	0.92	0.98

The IEEFO-CNN model performed best out of all of the above-mentioned architectures. IEEFO-CNN correctly recognized 292 users and rejected 299 impostors out of the test data set. It made only 9 errors in total. Clearly the additional improved optimization led to a much better tuning of the decision boundary for this model, resulting in much fewer false classifications.

As can be seen from the experimental results, authentication accuracy of the authentication system based on CNN also keeps increasing gradually with the improvement of optimization approaches. Despite being perfect in term of accuracy, the conventional CNN (the simple version of the CNN architecture) is far behind the performance of the optimization-based CNN architectures. While the accuracy of the conventional CNN is around 85.17%, the EEFO-CNN achieved 93.50% accuracy, i.e., it outperformed the CNN by 8.33% of accuracy. This shows that Electrical Eel Foraging Optimization can find the best hyper parameters for the CNN, leading to great performance. The proposed IEEFO-CNN is the best among all the models. It has the highest accuracy of 98.50%, i.e., an overall increase of 11%. In terms of false acceptance rate (FAR) and false rejection rate (FRR), performance increases gradually from CNN to EEFO-CNN and IEEFO-CNN, which means that with the optimization, the authentication system makes more accurate and reliable decisions.

E. Discussion of Authentication Metrics

The efficiency of the biometric authentication system depends on the accuracy and security of the recognition process. While the system guarantees the minimum of the classification error, the usability of the system depends on as low as possible rejection of the real users. Obviously, a low classification and rejection rates of the system does not mean that it is good. Instead, it can be concluded that the system requires evaluation of multiple metrics to characterize it effectively.

The traditional CNN produced the highest accuracy of the overall recognition process of approximately 87.50%, which indicated that this learning method is suitable for classifying emotion features from facial expressions. However, the CNN had a relatively high FRR of 22.33%, which means that the system may fail and deny the user entry to his/her account. The implementation of EEFO-CNN improved the system, which proved the effectiveness of optimization in achieving the best performance. As a result, the FRR was lowered to 6.67%, while the FAR was reduced to 1.67%, which is a significant improvement compared to conventional CNN.

The proposed IEEFO-CNN had the best trade-off between the security and usability of the authentication system—the recognition rate was 98.50%, FAR 0.33%, and FRR 2.67%. The overall security of the system covered by EER, which was 13.20% for CNN, 6.83% for EEFO-CNN, and 1.50% for IEEFO-CNN. The AUC values of the CNN, EEFO-CNN, and IEEFO-CNN were 0.89, 0.92, and 0.98, which means that the system distinguished between real and impostor users with very high accuracy.

F. Effect of Improved Electric Eel Foraging Optimization

The first one involves a series of upgrades on the Electric Eel Foraging Optimization algorithm. Adaptive energy factor control for instance helped strike a balance between exploration and exploitation which in turn helped the algorithm explore new terrains in the search space during early stages and exploit after convergence. The other improvement of learning is poor elite preservation and genetic diversity preservation to keep the good solution set throughout the learning process, dynamic migration and addition of Levy flight for stagnation reduction, hyper parameter optimization of CNN for better feature extraction and classification accuracy, and generalization to different facial expressions.

G. Security Implications of the Proposed Framework

Our pathological CAPTCHA framework is robust against presentation attacks and requires users to display facial expressions recognized by a facial emotion recognition system. Compared to static facial authentication, our framework offers increased resistance to presentation attacks by requiring a user to perform an action (i.e., changing their facial expression) when authenticating. The proposed online verification framework first includes two layers of authentication for online services: cognitive processes of information in the human brain and monitoring and verification of human behaviours. The pathological CAPTCHAs significantly impede automatic intrusion attempts. Even a simple CAPTCHA would become a very effective barrier to attackers who attempt to compromise the pathological CAPTCHA, because in addition to recognizing the CAPTCHA, the subsequent facial emotion verification also has to be correctly verified by the attacker. The false-acceptance rate (FAR)

of our verification framework for facial emotion verification even in the simple CAPTCHA case is as low as 0.33%.

H. Comparison with Existing Studies

Building a humanized authentication system is a trending topic, and we have witnessed myriad works done on CAPTCHA security, facial identity detection, CNN-based vision-driven emotion classification, and optimization strategies. Motivated by the fact that each process cannot provide the intended result on its own, we propose an omnibus intelligent humanoid authentication framework that converges CAPTCHA, facial emotion analysis, deep CNN classification, and intelligent ANN-based optimization to provide a robust solution to resist cyber-threats. The efficiency of our proposed framework is justified through promising results of performance benchmarks with 98.50% accuracy, an AUC of 0.98, 0.33% FAR, and 1.50% EER. Furthermore, incorporation of the improved EEFO algorithm has enriched the global cyber security and humanoid authentication research.

I. Discussion of Research Objectives

Based on the results, it can be inferred that all research goals are fulfilled for this research. The study designed a two-level CAPTCHA authentication system that consists of facial emotion recognition. It also enhanced the EEFO algorithm. The primary evaluation metrics were employed to quantify the performance of the improved system. The comparative analysis revealed that the IEEFO-CNN surpasses both CNN and EEFO-CNN in each of the evaluation metrics from all the angles. Hence, the integration of facial emotion recognition into the IEEFO-CNN authentication system finds a potential deployment in the social media, entertainment, and security-focused online platforms.

V. CONCLUSION

The IEEFO-CNN has been developed to carry out two level authentication using facial emotion recognition. This paper proposed the combination of the text-based CAPTCHA verification and behavioural biometric authentication for security against the attack of automated entities and unauthorized users. Improved Electric Eel Foraging Optimization that incorporated adaptive energy factor control, elite maintenance, dynamic migration and exploration assistance using Levy flight to optimize CNN hyper parameters has been developed.

The evaluation was performed using the data set of 2,000 facial images belonging to 500 individuals. The IEEFO-CNN performance measured authentication accuracy, FAR, FRR, EER, AUC and time at threshold value of 0.61 as 98.50%, 0.33%, 2.67%, 1.50%, 0.98 and 36.19 seconds respectively which show superiority to both CNN and EEFO-CNN. From this result, the proposed optimization greatly improved the efficiency of facial emotion recognition and authentication reliability. Hence, it has shown that CAPTCHA verification with facial emotion recognition can be designed as an efficient security frame work.

VI. LIMITATIONS AND FUTURE RESEARCH

Although the suggested system demonstrated promising outcomes but there are certain limitations. The number of emotion classes utilized is four and data was obtained under ideal environment which is not representative of real-world situations and the presence of factors such as changing light conditions, low quality cameras, use of facial accessories by the user and change in user behaviour could affect the classification. Moreover, it is dependent upon camera-enabled devices and needs further investigation for devices with limited resources.

Larger and varied data sets along with multi-modalities (voice, fingerprint etc.) would also be tested. This framework can also be used in different situations like real-world conditions. Transformation based deep architectures along with live detection and anti-spoofing approaches need to be considered for protection against deep fake and presentation attacks.

RECOMMENDATIONS

Stronger security frame works should be established to incorporate two levels authentication frame works involving the integration of CAPTCHA with behavioural biometrics. The proposed IEEFO-CNN framework may be adopted by the social media websites, online register, E-learning systems and other sensitive web applications. Further study of larger datasets and implementation of anti-spoofing framework is recommended.

REFERENCES

[1] Acien, A., Morales, A., Monaco, J. V., Vera-Rodriguez, R., & Fierrez, J. (2022). TypeNet:Deep learning keystroke biometrics. IEEE Transactions on Biometrics, Behavior, and Identity Science, 4(1), 57–70. https://doi.org/10.1109/TBIOM.2021.3112540

[2] Ali, H. N., & Al-Dabbagh, S. S. M. (2026). A systematic literature review on biometric
a. Authentication in mobile banking. F1000Research, 15, 5.
b. https://doi.org/10.12688/f1000research.173855.1

[3] Ali, M. H., Yousif, R., & Al-Khafaji, N. (2024). Hyper parameter optimization in deep learning Models using bio-inspired algorithms. Applied Soft Computing, 140, and 110278.

[4] Guerar, M., & Migliardi, M. (2022). Truth-seekers Chain: Leveraging invisible CAPPCHA, SSI and block chain to combat disinformation on social media.

[5] Gervasi, B. Murgante, S. Misra, A. M. A. C. Rocha, & C. Garau (Eds.), Computational Science And It's Applications – ICCSA 2022 Workshops (Vol. 13380, pp. 419–431). Springer International Publishing. https://doi.org/10.1007/978-3-031-10542-5_29

[6] Guerar, M., Verderame, L., Migliardi, M., Palmieri, F., & Merlo, A. (2021). Gotta CAPTCHA 'em all: A survey of 20 years of the human-or-computer dilemma. ACM Computing Surveys, 54(9), 192:1–192:33. https://doi.org/10.1145/3477142

[7] Gutub, A., & Kheshaifaty, N. (2023). Practicality analysis of utilizing text-based CAPTCHA Vs. graphic-based CAPTCHA authentication. Multimedia Tools and Applications, 82(30), 46577–46609. https://doi.org/10.1007/s11042-023-15586-5

[8] Khan, A., Sohail, A., Zahoora, U., & Qureshi, A. S. (2020). A survey of the recent architectures of deep convolutional neural networks. Artificial Intelligence Review, 53(8), 5455–5516. https://doi.org/10.1007/s10462-020-09825-6

[9] Noury, Z., & Rezaei, M. (2020). Deep-CAPTCHA: A deep learning based CAPTCHA solver for vulnerability assessment (No. arXiv: 2006.08296). arXiv. http://arxiv.org/abs/2006.08296

[10] See, A., Wingarz, T., Radloff, M., & Fischer, M. (2024). Detecting web bots via mouse Dynamics and communication metadata. In N. Meyer & A. Grocholewska-Czuryło (Eds.), ICT Systems Security and Privacy Protection (pp. 73–86). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-56326-3_6

[11] Tariq, N., Khan, F. A., Moqurrab, S. A., & Srivastava, G. (2023). CAPTCHA types and Breaking techniques: Design issues, challenges, and future research directions (No. arXiv: 2307.10239). arXiv. http://arxiv.org/abs/2307.10239

[12] Trong, N. D., Huong, T. H., & Hoang, V. T. (2023). New cognitive deep-learning CAPTCHA. Sensors, 23(4), 2338. https://doi.org/10.3390/s23042338

[13] Turay, T., & Vladimirova, T. (2022). Toward performing image classification and object detection with convolutional neural networks in autonomous driving systems: A survey. IEEE Access, 10, 14076–14119. https://doi.org/10.1109/ACCESS.2022.3147495

[14] Wang, X., Zhang, Y., & Li, S. (2023). Electric Eel Foraging Optimization (EEFO): A novel Met heuristic algorithm for global optimization. Information Sciences, 640, 119913.

[15] Wang, Y., Wei, Y., Zhang, M., Liu, Y., & Wang, B. (2021). Make complex CAPTCHAs Simple: A fast text CAPTCHA solver based on a small number of samples. Information Sciences, 578, 181–194. https://doi.org/10.1016/j.ins.2021.07.040

[16] Zhang, L., Han, G., & Kumar, N. (2023). Recent advancements in CNN hyper parameter tuning Using met heuristics: A review. Expert Systems with Applications, 216, 119406.

[17] Zhao, W., Wang, L., Mirjalili, S., Khodadadi, N., & Cao, Q. (2024). Electric eel foraging Optimization: A new bio-inspired optimizer for engineering applications. Expert Systems with Applications, 238, 122200. https://doi.org/10.1016/j.eswa.2023.122200