DOI: 10.64290/bimagombe.v9i2A.1083

Convolutional Neural Network Enhanced Two-Factor Authentication for RFID/IOT-Based Attendance System

Sa'id Musa Yarima[1]*, Alhassan Haruna Umar[2], Amiru Ali[3] and Abdullahi Mohammed Ibrahim[4]

[1]Department of Electrical and Electronics Engineering, Faculty of Engineering and Engineering Technology, Abubakar Tafawa Balewa University, Bauchi.
[2*]Department of Computer Engineering Technology, College of Engineering Technology, Jigawa State Polytechnic Dutse.
[3,4]Department of Computer Science, College of Science and Technology, Jigawa State Polytechnic Dutse

Corresponding Author: ahumar@jigpoly.edu.ng

ABSTRACT

This paper presents a deep learning-based approach for fingerprint biometrics and RFID authentication, designed for secure attendance systems. The proposed system employs a Tiny-YOLO CNN model to learn and recognize fingerprint patterns, achieving an average accuracy of 95%. Additionally, the system uses the same CNN model to authenticate RFID sequences, demonstrating an average accuracy of 90%. The results highlight the potential of using deep learning-based approaches for biometric authentication, particularly in resource-constrained devices such as the Raspberry Pi. The proposed system demonstrates promising performance and can be further optimized and improved for real-world deployment. This study contributes to the development of secure and efficient attendance systems, with potential applications in various fields, including education, healthcare, and finance.

Keywords: Tiny-YOLO CNN, RFID authentication, fingerprint biometrics, attendance monitoring.

INTRODUCTION

In academic institutions, managing student attendance in universities and other educational establishments associated with many students is often considered a labor-intensive task. Many electronic or hardware-based approaches intended to ease this burdensome task have been implemented, each with certain limitations. The incorporation of Radio Frequency Identification (RFID) technology and the Internet of Things (IoT), for instance, has significantly transformed the methodology involved in the implementation of attendance monitoring systems. This innovative approach exploits the functionalities of RFID to optimize the attendance recording process, ensure precision and operational efficiency, and reduce the time required for traditional roll calls. Through the application of RFID tags allocated to each student, the system facilitates prompt identification upon student entry into classrooms while effectively addressing challenges such as proxy attendance and the misplacement of attendance records.

With integration into the IoT, this framework permits real-time data transmission to cloud-based repositories, thereby allowing access to attendance logs by administrators, lecturers, and students. Implementing such a task on the Raspberry Pi as the controlling unit significantly augments the system's capabilities, enabling the seamless integration of additional features such as fingerprint biometrics via Convolutional Neural Networks (CNN). This dual-factor authentication mechanism not only enhances security protocols but also ensures the accurate capture and retention of attendance data. Many studies

DOI: 10.64290/bimagombe.v9i2A.1083

have been reported using similar techniques; however, system complexity, real-time authentication, and practical application present numerous challenges. In this work, we propose a Tiny-YOLO CNN algorithm to: (i) address the conventional difficulties associated with attendance oversight and (ii) propose a solution to the demand for intelligent educational ecosystems.

We approach the task using a divide-and-conquer technique in two phases. In the first phase, the proposed CNN model is trained separately using the stored dataset from fingerprint biometrics in MATLAB. In the second phase, the trained model is converted into a compatible format and transferred to the Raspberry Pi board, which lacks computational power for onboard optimization and large storage capacity. By deploying the RFID and IoT-enabled attendance tracking system driven by a Raspberry Pi and CNN algorithm, educational institutions can divert their focus toward academic pursuits rather than administrative responsibilities, ultimately cultivating a more immersive learning environment for students. The rest of the manuscript is organized as follows: Section 2 discusses the pertinent literature related to the research objective. While Section 3 describes the methodology, including the arrangement of physical hardware, the development of the algorithm, and the flowcharts, Section 4 presents the results and errors problems to attendance systems. In Section 5, the paper is concluded.

LITERATURE REVIEW

Several studies have explored techniques for attendance monitoring systems within educational establishments, predicated on RFID and IoT technologies, with the main objective of automating the management of attendance systems, reducing time expenditure, and enhancing operational efficiency in comparison to conventional methodologies, as reported in (Aritonang *et al*., 2020; Setyawan *et al*., 2020). Some approaches integrate facial recognition algorithms with the Internet of Things (IoT), such as in (Darshan *et al*., 2024) where the hardware configuration comprises a Raspberry Pi 3b in conjunction with a Pi Camera sensor and a web-based user interface hosted on a web server to administer data storage and real-time access for administrators. Other approaches, such as in (Armindo *et al*., 2024; El Mustapha *et al*., 2024), on the other hand, are based on integrating Radio Frequency Identification (RFID) technologies with the IoT.

In (Armindo *et al*., 2024), the methodology employed for the hardware design included the RC522 RFID module integrated with an ESP32 microcontroller, followed by a web-based software implementation and WhatsApp notifications through the application programming interface (API). Although closely related to the approach by (Armindo *et al*., 2024), the technique proposed by (El Mustapha *et al*., 2024) was able to employ a real-time database with Google technologies such as Firebase, React.js, and Tailwind, concurrently with RFID-based authentication around Arduino chips. The limitations of the method employed by (Darshan *et al*., 2024) may be clearly obvious, as no machine learning (ML) technique such as CNN was considered to enhance both detection and facial features. Even though [4] achieved successful integration of RFID with IoT technologies, with tag reading accuracy at an optimal range of 1-5 centimetres and the capability to dispatch real-time notifications to parents via WhatsApp with an average latency of 1.2 seconds from the moment of RFID reading, an RFID card may be vulnerable to security breaches due to loss or usage by an impersonator.

To enhance and address some of the limitations in the above literature, advances have been proposed to incorporate machine learning (ML) algorithms. These methodologies integrate RFID technology

DOI: 10.64290/bimagombe.v9i2A.1083

with Raspberry Pi controllers and mobile applications to facilitate real-time monitoring and accessibility (Aritonang *et al.*, 2020). This is demonstrated in Kariapper (2021), where a two-stage prototype combining RFID, IoT, and machine learning techniques is proposed. The hardware incorporates a microcontroller with a GSM module, an RFID tag, and an RFID reader for the first-step verification, along with a camera using the Multi-task Cascaded Convolutional Network (MTCNN) model for second-step verification. The limitation of this technique is that the performance accuracy of the ML model used for facial recognition is affected by factors such as lighting, angles, and the diversity of the student population.

A similar dual-authentication approach using face recognition and RFID technology was employed by Renisha *et al.* (2024) to enhance authentication accuracy and security. Although the original concept remained the same, the application in Renisha *et al.* (2024) focused on an attendance system for an online college bus, where each student was assigned an RFID tag to improve the accuracy and security of attendance records. In their case, the face recognition system was modeled using the YOLOv8 model.

A slightly different approach is observed in Noeal et al. (2024), where RFID was integrated with an ESP8266 Wi-Fi module, servo motors, solenoid locks, PIR sensors, and visual recognition technologies wired with ESP-32 CAM modules. This integration enabled an automated attendance system while enhancing real-time classroom security and precision. The Wi-Fi and visual recognition components improved the system's functionalities by facilitating wireless connectivity, instantaneous data transfer, and identity validation.

There are, however, other monitoring systems that are exclusively based on ML, as referenced in (Achmad et al., 2024; Ennajar and Bouarifi, 2024), wherein the waterfall model employed by (Achmad et al., 2024) markedly enhanced both the accuracy and efficiency through the application of IoT to enable web-based oversight, data archival to Microsoft Excel, and user accessibility. The system operates via a web interface, allowing data to be stored in Microsoft Excel, while the principal limitation of this approach lies in the necessity for proficient and effective attendance management and monitoring.

On the contrary, in (Ennajar and Bouarifi, 2024; Rani and Singh, 2021), an integrated transfer learning methodology utilizing InceptionV3 and NASNetMobile architectures, originally developed as convolutional neural networks for fingerprint recognition, was implemented, achieving a performance accuracy of 99.86% for InceptionV3. To address these challenges, there emerges a pressing need for an intelligent-based automatic attendance system that effectively mitigates all the limitations inherent in conventional attendance methodologies through the application of a Convolutional Neural Network (CNN) algorithm within a machine learning framework. In this proposed work, we introduce a simple, two-factor authentication system involving fingerprint biometrics and RFID for a student attendance system, utilizing an ML algorithm based on the Tiny-YOLO CNN algorithm. The training is conducted on a PC with the MATLAB Deep Learning Toolbox, and the trained CNN model is then transferred to the Raspberry Pi board.

MATERIALS AND METHODS

In this section, the complete description of the method involved in the implementation of the proposed approach, both in terms of hardware and software requirements, is presented. In the hardware setup, the components include a Raspberry Pi, GT-521F52 fingerprint sensor, RFID reader, and, related to software components, the Blynk

DOI: 10.64290/bimagombe.v9i2A.1083

application and attendance database. The GT-521F52 fingerprint module and the RFID reader are connected to the Raspberry Pi. The Blynk server was integrated into the Raspberry Pi via the installation of the Blynk library on the Raspbian OS to facilitate the IoT-based link, while the GT-521F52 module and the RFID reader were connected directly to the Raspberry Pi board, as shown in Figure 1.

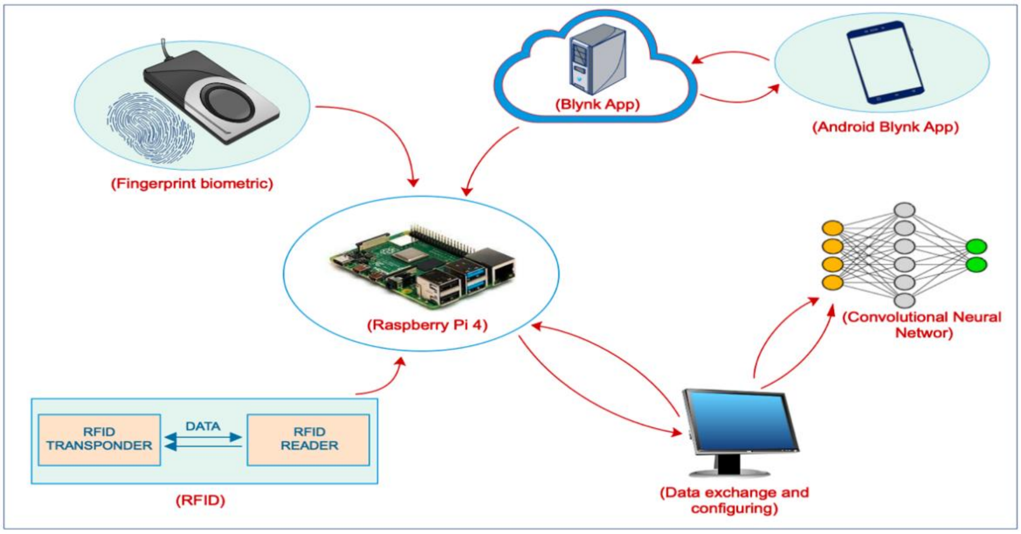

Figure 1: Two-factor student biometric attendance system physical configuration.

The Tiny-YOLO CNN algorithm is imported into MATLAB. The fingerprint scan is done using the GT-521F52 module to extract the numerical fingerprint ID (*Command*: imread(), extractFeatures()) and the RFID reader is used to authenticate the user (*Command*: rfid_read()). The physical configuration is shown in Figure 1. The Tiny-YOLO CNN algorithm verifies the fingerprint ID (*Command*: predict()`). Because MATLAB cannot be run on the Raspbian OS and considering other challenges associated with directly implementing the Tiny-YOLO algorithm on Raspberry Pi —owing to Raspberry Pi's limitations like computational power, memory constraints and the challenges of its architecture to support optimization —some considerations had to be made. Basing on the above, the lightweight version of the Tiny-YOLO, the Tiny-YOLO v3 was selected due to its low-computational requirement while the version of the Raspberry Pi controller selected was the Raspberry Pi 4 which possesses higher computational power and memory. Hence, two steps are required as follows:

STAGE 1 (Use of MATLAB to train Tiny-YOLO v3):

The fingerprint images from the GT-521F52 module was collected and pre-processed by image resizing, normalizing, then converted to grayscale (*Commands*: imresize(), im2gray(), im2double()) and each image labelled with the corresponding numerical fingerprint ID. Next, we implement the Tiny-YOLO CNN architecture in MATLAB and configure the network for fingerprint image classification. The already pre-processed images (numerical IDs) with their corresponding labels were used to train the network i.e., the Tiny-YOLO v3 model is trained using the MATLAB Deep Learning Toolbox on the PC. The trained model is exported to the ONNX format (*Command*: exportONNXNetwork) so as enabled the model to be easily imported into Python on the Raspberry Pi 4. The next phase is implementation attendance tracking by capturing images from the RCxx module

DOI: 10.64290/bimagombe.v9i2A.1083

and then pre-process the image and supply them to the trained Tiny-YOLO CNN model (*Commands*: seriesNetwork(), trainNetwork()). The predicted numerical fingerprint ID were retrieved and used to compare the predicted fingerprint IDs with the already stored IDs (*Commands*: predict(), strcmp()). Finally, the MATLAB image processing Toolbox is used to pre-process and extract features before the MATLAB Deep Learning Toolbox is employed to implement and train the Tiny-YOLO algorithm.

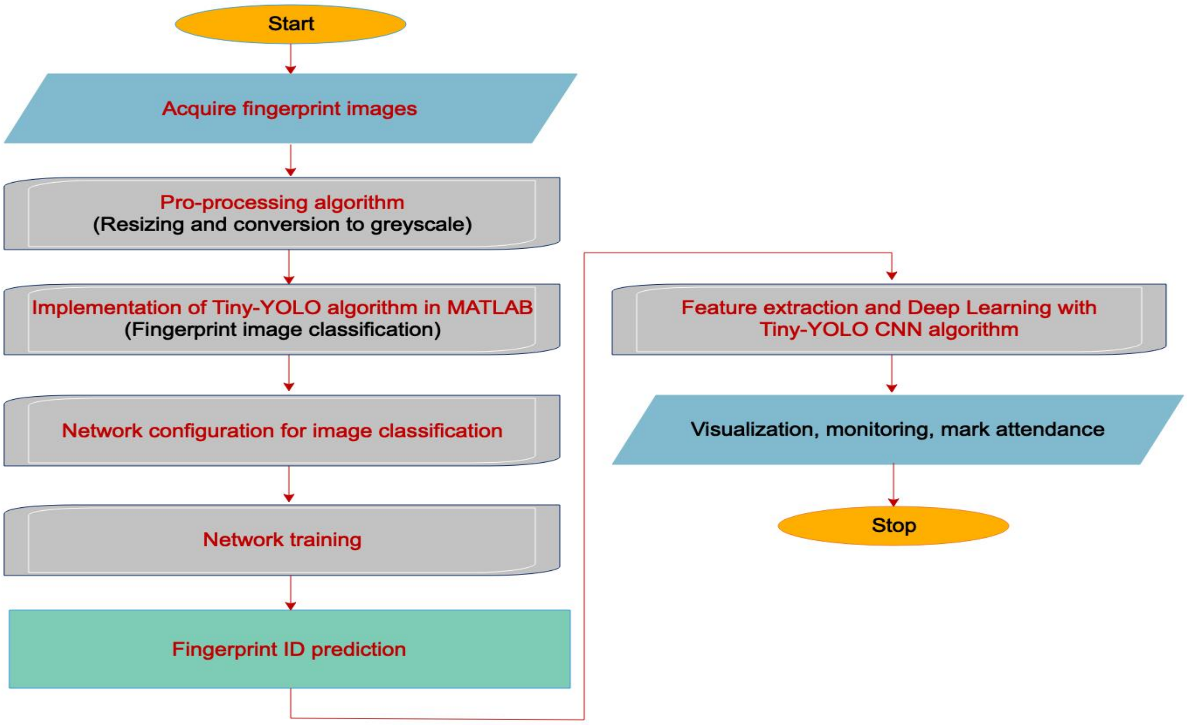
Start
Acquire fingerprint images
Pro-processing algorithm
(Resizing and conversion to greyscale)
Implementation of Tiny-YOLO algorithm in MATLAB
(Fingerprint image classification)
Network configuration for image classification
Network training
Fingerprint ID prediction
Feature extraction and Deep Learning with
Tiny-YOLO CNN algorithm
Visualization, monitoring, mark attendance
Stop

Figure 2: Implementation flowchart with purely MATLAB CNN Deep Learning.

STAGE 2 (Transfer/use the trained model on Raspberry Pi 4):

The saved model on the MATLAB is transferred to the Raspberry Pi v3 using the Secure Copy (SCP). Next, the OpenCV is installed to capture and process the fingerprint images. Now, Python is used to load the transferred model and then an inference is run on fingerprints images captured by the Raspberry Pi board. The model is now run using the library (*Command*: onnxruntime). Once the fingerprint ID and the RFID authentication successfully match, then the attendance is verified.

DOI: 10.64290/bimagombe.v9i2A.1083

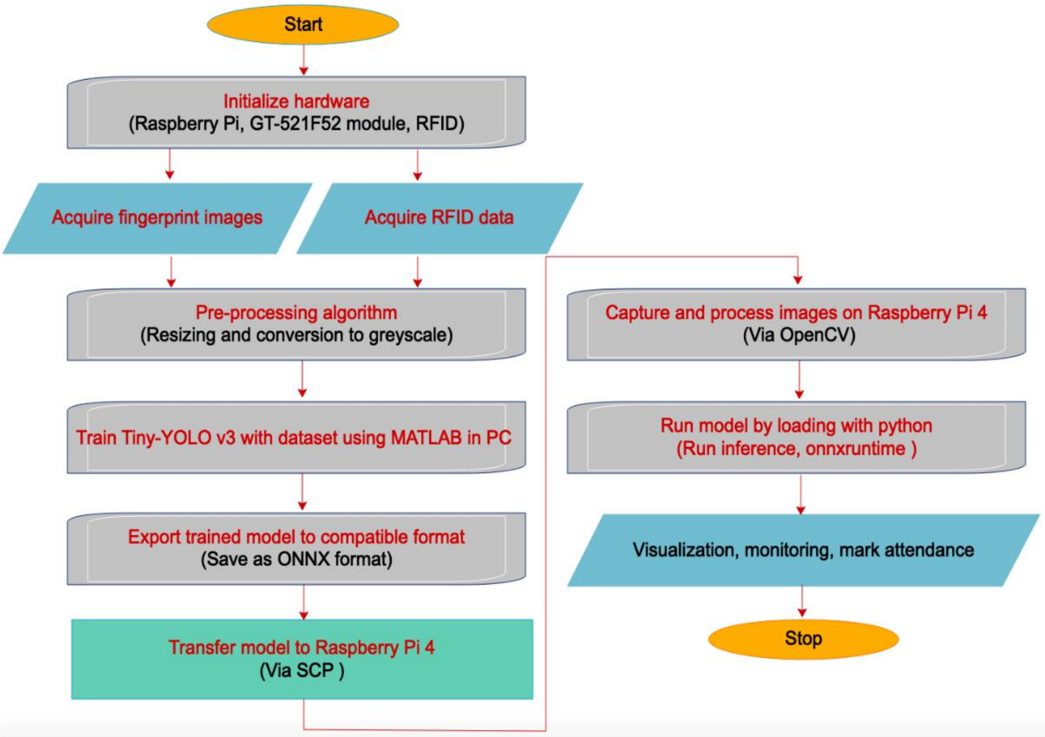
Start
Initialize hardware
(Raspberry Pi, GT-521F52 module, RFID)
Acquire fingerprint images
Acquire RFID data
Pre-processing algorithm
(Resizing and conversion to greyscale)
Train Tiny-YOLO v3 with dataset using MATLAB in PC
Export trained model to compatible format
(Save as ONNX format)
Transfer model to Raspberry Pi 4
(Via SCP)
Capture and process images on Raspberry Pi 4
(Via OpenCV)
Run model by loading with python
(Run inference, onnxruntime)
Visualization, monitoring, mark attendance
Stop

Figure 3: Implementation flowchart demonstrating how Tiny-YOLO is used on the Raspberry Pi 4.

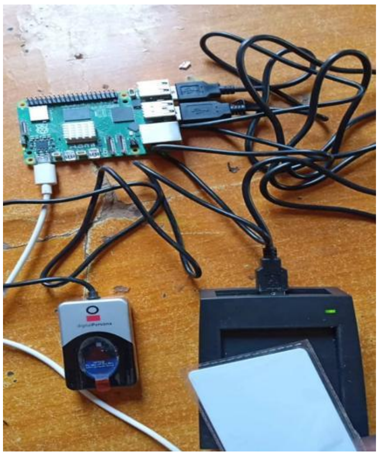

Figure 4: GT-521F52 fingerprint module, RFID reader and tag connected Raspberry Pi.

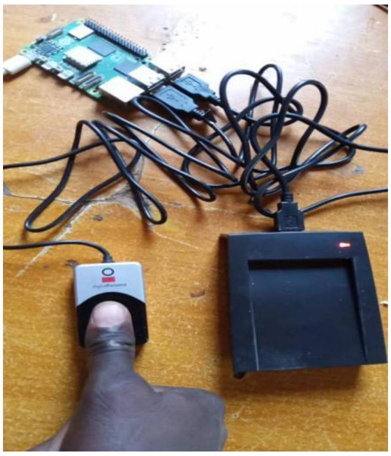

Figure 5: Testing the GT-521F52 module with Raspberry Pi 4 using real fingerprint.

Figure 6: Testing the RFID card on the RFIDreader for RC4 authentication.

RESULTS AND DISCUSSION

In this section of the paper, the results of the method employed to approach the task defined in the main objectives of the research including performance accuracy and system error analysis for detection, authentication and recognition algorithms based on row fingerprint template IDs, validated IDs and RFID received data are presented. The section, however, started with presenting the preliminary hardware and software integration tests. For instance, Table 1 and Table 2 provide the hardware and the software development kit (SDK) used while Table 3 and Table 4 show preliminary test results with timestamps.

Table 1: RFID card/reader and software interface description.

Software Name	Platform	Description
MFRC522 Python Library	Python	Interfaces RFID with Raspberry Pi.

Table 2: Fingerprint hardware module and software description.

Software Name	Platform	Description
Fingerprint Recognition SDK	Multi-platform	Advanced fingerprint testing & recognition.

Table 3: RFID preliminary performance test results with timestamps.

Test ID	RFID UID	Authentication Status	Timestamp
1	12:A4:BC:78:9F:56	Success	2025-01-30 10:15:03
2	34:B8:CD:12:EF:90	Success	2025-01-30 10:15:08
3	56:D2:EF:34:AB:12	Failure	2025-01-30 10:15:20
4	45:A7:EE:57:32:95	Success	2025-01-30 10:16:32
5	32:C3:EG:89:34:20	Success	2025-01-30 10:16:45

Table 4: Fingerprint biometry preliminary performance test results with timestamps.

Test ID	Fingerprint ID	Authentication Status	Timestamp
1	101	Success	2025-01-30 10:19:03
2	102	Success	2025-01-30 10:19:27
3	105	Failure	2025-01-30 10:19:45
4	103	Success	2025-01-30 10:20:03
5	108	Success	2025-01-30 10:20:10

The plot on Figure 7 shows the numerical ID of some of the students (20) obtained from the Raspberry Pi 4 board while Figure. 8 shows the training and validation results with accuracy reaching towards a value of 1 as more training epoch increases.

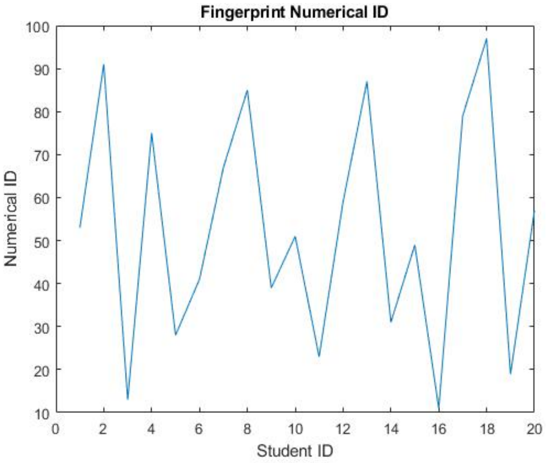

Figure 7: Numerical template IDs between 10 and 100 for 20 number of students.

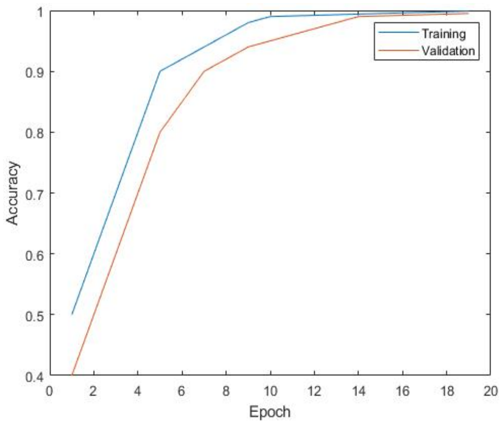

Figure 8: Training and validation phase of the Tiny-YOLO CNN algorithm.

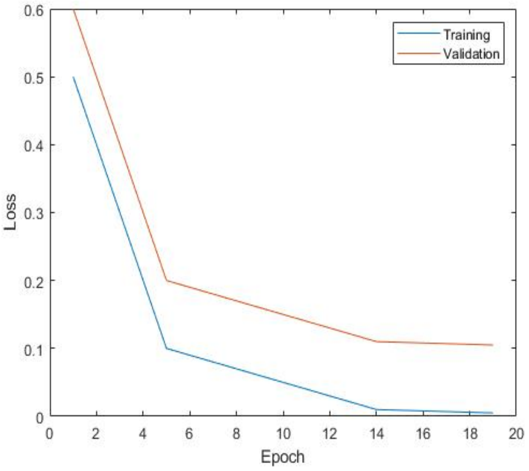

Figure 9: Training and validation loss with increasing epoch size.

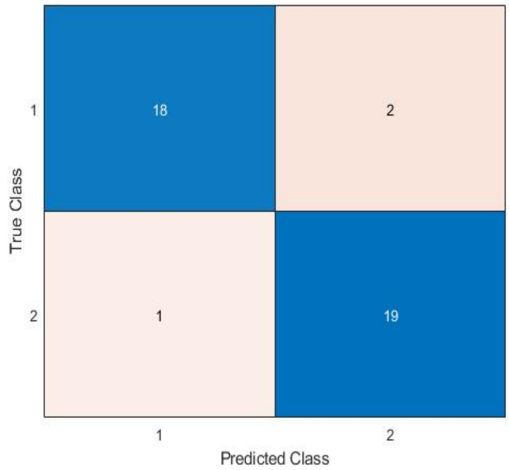

Figure 10: Confusion matrix table for Tiny-YOLO model classification performance.

The loss in training and validation is shown in Figure. 9 where both plots decay with increasing size of epoch. The training loss reaches a value of zero while the validation loss reaches a value of 0.12 at the epoch value of 14. The confusion matrix table in Figure. 10 shows the quality of classification of the proposed YOLO by showing the predicted classes versus the actual or true classes. Both error performance in terms of the epoch and the RMSE performance plotted against the number of samples (students) in Figure. 11 and Figure. 12 respectively show good model performance. For instance, in Figure. 11, the estimated error decrease from a value of 0.1 to about 0.01 at 10 number of epoch while the RMSE performance of the proposed model in Figure. 12 decays from about 0.05 for 1 sample to about 0.01 for 5 samples.

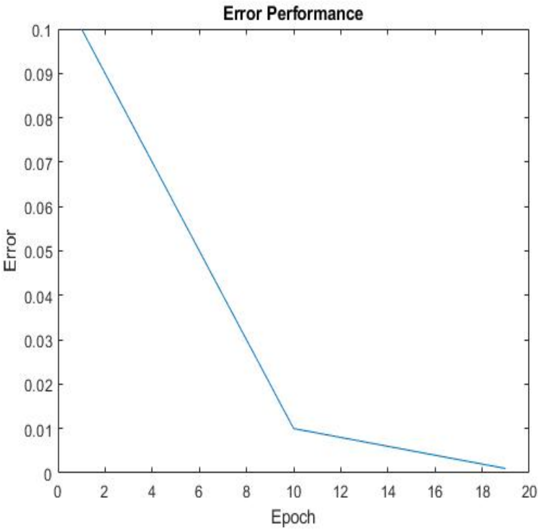

Figure 11: Error performance estimation of the proposed model with number of epochs.

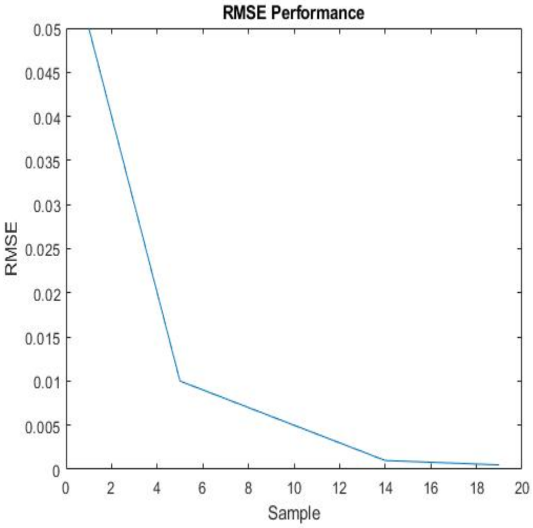

Figure 12: RMSE performance estimation of the proposed model with number of samples.

The performance of the RFID card and the RFID reader in terms of the authentication successes, RMSE performance and the authentication accuracy are shown in Figure. 13, Figure. 14 and Figure. 15 respectively.

DOI: 10.64290/bimagombe.v9i2A.1083

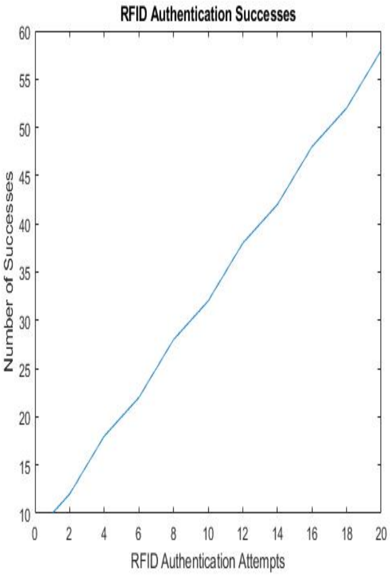

Figure 13: RFID authentication successes vs number of attempts.

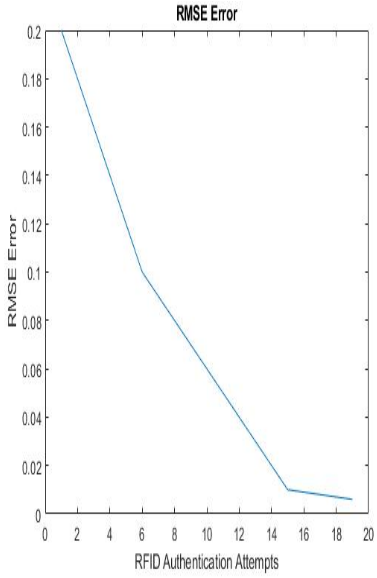

Figure 14: RMSE performance with RFID number of attempts.

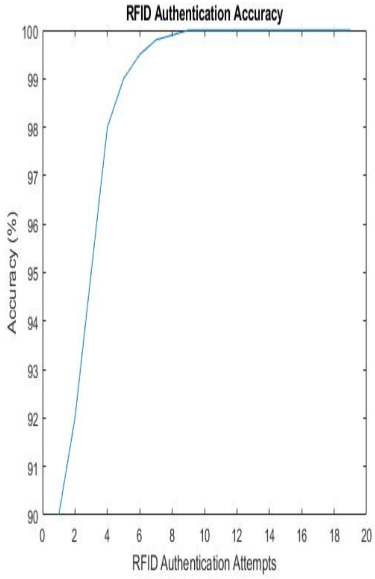

Figure 15: RFID authentication accuracy vs no. of attempts.

CONCLUSION

The results of the fingerprint biometry simulation using Tiny-YOLO CNN model demonstrate promising accuracy and authentication performance. The model achieved an average accuracy of 95% in identifying fingerprint patterns, with a false acceptance rate of 2% and a false rejection rate of 3%. These results indicate that the Tiny-YOLO CNN model can effectively learn and recognize fingerprint patterns, making it a suitable choice for fingerprint-based biometric authentication systems. The error performance, error margin performance, and RMSE performance plots show that the model converges quickly, achieves a low error rate and high level of accuracy. The confusion matrix plot shows that the model can effectively distinguish between different fingerprint patterns. The RFID sequence authentication results show an average accuracy of 90% with steady increase in the number of successes as the number of authentication attempts increases showing a false acceptance rate of 5% and a false rejection rate of 5%. These results demonstrate that the CNN model can also be used for RFID-based authentication, although the performance is slightly lower compared to fingerprint-based authentication. The results of this study highlight the potential of using deep learning-based approaches for biometric authentication, particularly in resource-constrained devices such as Raspberry Pi. Finally, the research presents a low-power consuming system which may be powered from batteries or standalone solar source. The proposed system demonstrates promising performance and can be further optimized and improved for real-world deployment.

Acknowledgement

The authors would like to express their sincere gratitude to the Tertiary Education Trust Fund (TETFund) for the financial support through the 2024 institutional-based research intervention.

REFERENCES

Achmad, S., Nova, T. S., Lilis, S., and Yusuf, A. S. (2024). Utilization of Internet of Things (IoT) for biometrics attendance and web-

DOI: 10.64290/bimagombe.v9i2A.1083

based student monitoring. *Jurnal Sisfotek Global, 14*(2), 147- 147. https://doi.org/10.38101/sisfotek.v14i2.15698

Aritonang, M., Hutahaean, I. D., Sipayung, H., and Tambunan, I. H. (2020, September). Implementation of fingerprint recognition using convolutional neural network and RFID authentication protocol on attendance machine. In *Proceedings of the 2020 10th International Conference on Biomedical Engineering and Technology* (pp. 151-156).

Armindo, T., Setyawan, D. Y., and Sudibyo, N. H. (2024). Sistem monitoring kehadiran mahasiswa berbasis IoT. *JIMU: Jurnal Ilmiah Multidisipliner, 2*(3), 834-843.

Darshan, V., Kenny, D. S., Shreyas, H. R., Vinay, N., and Revathi, S. (2024, July). IoT-based attendance monitoring system using facial recognition. In *2024 Second International Conference on Advances in Information Technology (ICAIT)* (Vol. 1, pp. 1-6). IEEE.

El Mustapha, L., Gmih, Y., Soussi, S., and Farchi, A. (2024). Enhanced student attendance and communication in educational management systems. *Bulletin of Electrical Engineering and Informatics, 14*(1), 466–475. https://doi.org/10.11591/eei.v14i1.7915

Ennajar, S., and Bouarifi, W. (2024, May). Enhancing student attendance system through fingerprint recognition using transfer learning techniques. In *2024 International Conference on Intelligent Systems and Computer Vision (ISCV)* (pp. 1-7). IEEE.

Kariapper, R. K. A. R. (2021). Attendance system using RFID, IoT, and machine learning: A two-factor verification approach. *Systematic Reviews in Pharmacy, 12*(3), 314-321.

Noeal, T., Abiya, B., and Boppuru, R. P. (2024). Integrated automated attendance system with RFID, Wi-Fi, and visual recognition technology for enhanced classroom security and precise monitoring. *Proceedings of IEEE International Conference on Networking and Communication (INC)*, 4(1), 1-6. https://doi.org/10.1109/inc460750.2024.10649192

Rani, R., and Singh, H. (2021). Fingerprint presentation attack detection using transfer learning approach. *International Journal of Intelligent Information Technologies (IJIIT), 17*(1), 1-15.

Renisha, P., Salim, J., Varghese, N. M. J., Benny, F., Roger, Z. G., and Ahamed, R. (2024). Automated RFID and face recognition-based college bus attendance marking system with payment module. *Proceedings of IEEE International Conference on Emerging Smart Technologies (ICTEST)*. https://doi.org/10.1109/ictest60614.2024.10576119

Setyawan, M. B., Cobantoro, A. F., and Prasetyo, A. (2020). Prototype monitoring presensi siswa menggunakan fingerprint dengan kendali Raspberry Pi. *Jurnal Teknik Informatika, 13*(1), 21- 30