Active Gait System for Real-Time Surveillance Against Cyber-Physical Attacks

Glen Lehlohonolo Moepi and Topside Ehleketani Mathonsi
Department of Information Technology, Tshwane University of Technology, Pretoria, South Africa

MoepiGL@tut.ac.za
MathonsiTE@tut.ac.za

Abstract: Cyberterrorism, espionage, and warfare are serious threats to national security. These attacks can harm people or destroy critical infrastructures like the data centres, computer networks, and systems. Surveillance systems currently used in monitoring critical infrastructures, national key points, and military exclusion zones (MEZ) are ineffective in detecting unauthorised intrusions. These issues compromise the stability of the countries, and the safety of the citizens and result in the loss of important assets. This experimental research study developed a Cyber Physical Security (CPS) defense gait-recognition monitoring system. Autonomous Machine Learning (ML) technology was employed to enhance the precision and reliability of the system against CPA, in tracking access, managing security clearances, and triggering alerts in the event of unauthorized entries to restricted areas.

Keywords: Cyber Physical Security (CPS), Deep Learning (DL), Gait analysis, Gait event detection, Machine Learning (ML)

1. Introduction

Power grids, necluear plants, and critical computer networks are currently facing the challenges of physical attacks. A study by Wlazlo *et al.* in (2021) and (Tyagi & Sreenath, 2021), shows that Cyber-Physical Attacks (CPA) are on the rise. Token-based and knowledge-based identification schemes are commonly used for verification when granting entry and security clearance to restricted areas. However, physical tokens can be cloned and are also susceptible to theft. In mitigation to that, the introduction of biometric systems can be used for security in authorization and intrusion detection systems (Robb, 2022).

Moro *et al.* (2022), compared Markerless and Marker-Based Gait Analysis, and it was determined that gait-recognition technology exhibits a high level of reliability and efficacy in accurately identifying individuals, achieving an accuracy rate of up to 99%. A different study by (Lin *et al.,* 2023) proved that the accuracy and dependability of systems used for authorizations can be increased by utilising gait recognition technology. The gait recognition technology in conjunction with Artificial Intelligence (AI) has been used successfully in surveillance (Yan *et al.*, 2021).

To reduce the risk of CPA and efficient administration of authorizations, this paper proposes an active gait recognition system using (ML). The paper seeks to provide a highly accurate and secure method of tracking authorized and detecting un-authorized individuals by using unique gait patterns. This paper endeavours to make a sizeable contribution to the domains of access and authentication systems.

The following is the order in which this paper is organized: Section 1, introduces gaits, AI and ML applications, the objectives of the study, the problem being addressed, and the paper's contributions. Section 2 highlights the related work on gaits systems. In Section 3, this paper experimented with the use of the proposed gait system. Section 4, brings the paper to a close with the results analysis and makes recommendations for future research.

2. Related Work

A research study by (Álvarez-Aparicio *et al.,* 2022) investigated the use of gait recognition technology as a means of biometric recognition. The study found that gait recognition technology can achieve high levels of accuracy, with an equal error rate of 1.4%. The study also showed that gait recognition technology can be used in real-time scenarios, making it a reliable option for authorization and intrusion detection. Similar to the study, this paper used the active gait recognition system and for real-time authorization and intrusion detection system (IDS) that will trigger alarms upon the detection of anomalies, a probable deterrent to intruders.

A surveillance detection study by (Esan et al., 2023), proved that Deep Learning (DL) technique model has 95% accuracy in anomaly detection. Their study combined Convolutional Neural Network (CNN) and Long Short-Term Memory (LSM). Another study by (Albuquerque *et al.,* 2021), also proved that the use of AI and gaits technology is effective in wide areas and long distances object identification. Similar to this study, DL is a fundamental element in object learning and anticipating normal gaits actions in high-risk facilities and effective management

of assets. Overall, the gait recognition technology has the potential to revolutionize authorization and intrusion detection systems.

Another study by (Lee & Tang, 2021), proposed a portable system for gait phase detection using AI. The system was designed to be used in healthcare settings, but the technology can be applied in access systems. The study showed that the proposed system achieved an accuracy of 91.3% in gait phase detection. Another embedded system was designed by (Pradel *et al.,* 2019) to analyze gait patterns and provide feedback to patients and healthcare providers. These studies showed that the systems were able to accurately measure gait parameters. The embedded gait analysis system proposed by (Pradel *et al.,* 2019) could be used to identify abnormal gait patterns in employees and livestock, which could be an indication of injury or fatigue; or animal is under attack. However, using embedded systems, digital wearables, and accelerometers is costly for a with many assets to track and monitor. This paper seeks to develop a system that is not cost-prohibitive, using a standard video camera and unsupervised clustering DL techniques.

3. Proposed Solution

The identity verification is implemented as part of the gait recognition using five different authentication sets. Each authorization is based on a set of following processes according to the technique. The proposed protocol includes several elements, such as:

- Acquiring gait characteristics.
- Extraction and processing of gait features.
- Reduced feature count.
- ML methods for classification.
- Depending on the outcomes of the categorization.

These processes enable reliable authentication that improves the gait-recognition system's security and usability as illustrated in Figure 1.

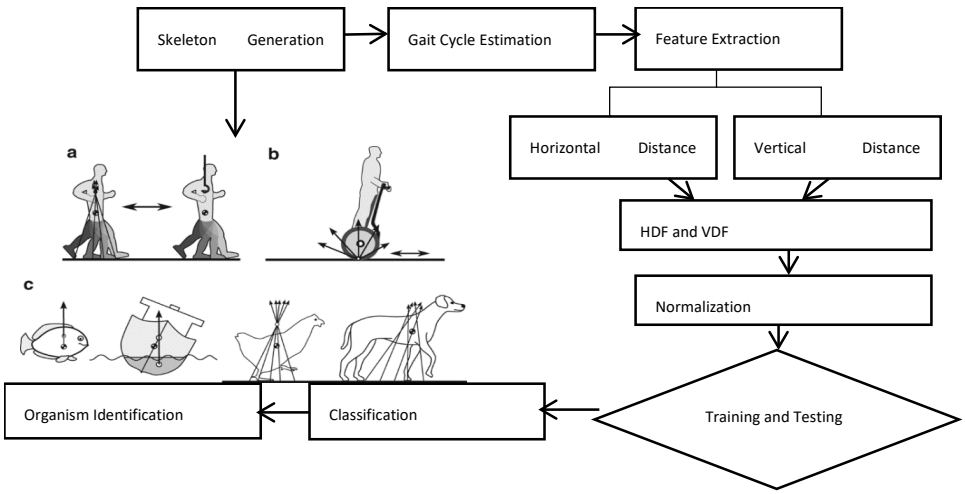

Figure 1: Active Gait System Architecture Design Incorporated (Maus, *et al.,* 2012)

4. The Implementation of the Proposed Scheme

A controlled environment setting for experimentation was established. A format for trial-and-error testing was employed with the Intersection over Union (IoU) ratio, as a cutoff point for assessing the object-detection models' accuracy. The region of overlap between the ground reference bounding box and the anticipated bounding box is the numerator. The area of union, or the region covered by both bounding boxes, served as the denominator.

Stage1: Webcam Object Detection

YOLOv4 is extremely effective in object identification technology. As depicted in Figure 2, YOLOv4 uses a deep Convolutional Neural Network (CSPDarknet53), a more sophisticated backbone network. With the help of this network design, YOLOv4 is better able to properly recognize objects by extracting more specific and discriminative information from the input image. Additionally, YOLOv4 uses several optimization approaches to boost its accuracy and speed. A good example of this is the incorporation of cross-stage partial connections

(CSP), which increase data flow and make it easier to interchange both high-level and low-level characteristics, improving detection performance. In order to properly handle objects of various sizes, YOLOv4 additionally makes use of the PANet (Path Aggregation Network) and Spatial Pyramid Pooling (SPP) modules.

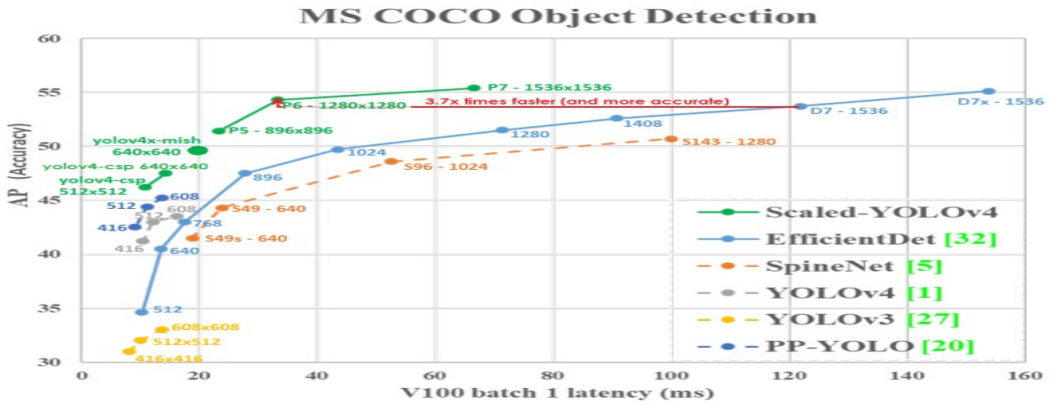

Figure 2: Object detection

1. Import Dependencies

Importing dependencies allows access and use of external libraries, modules, or frameworks that provide the necessary functionality and tools. The importation of specific dependencies serves two main purposes: enabling the execution of YOLOv4 object detection and leveraging the capabilities of Google Colab. To perform YOLOv4 object detections on a webcam, necessary learning dependencies include deep learning frameworks such as TensorFlow or PyTorch, which provide the necessary tools for building and training neural networks. Google Colab is a cloud-based platform that offers a hosted Jupyter notebook environment with access to computational resources, including GPU acceleration.

2. Cloning and Setting up a Darknet for YOLOv4

Cloning and setting up Darknet for YOLOv4 using AlexeyAB's darknet repository provides the necessary framework for implementing and running YOLOv4 object detections. AlexeyAB's darknet repository is ideal for its comprehensive implementation of YOLOv4 and its compatibility with different hardware platforms.

3. Adoption of Darknet for Python

Darknet for Python involves importing and utilizing pre-built functions from the darknet.py module. This allows seamless integratation of YOLOv4 functionality into the Python code, to perform object detections and work with the YOLOv4 model efficiently.

4. Helper Functions

Helper functions for image type conversion ensures compatibility and consistency between different image formats.

4.1 The Gait Recognition System Function Outputs

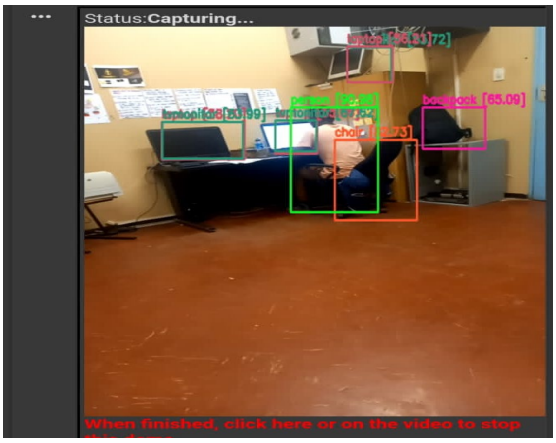

Figure 3: Object Detection YOLOv4

Using Yolo each frame of a video is treated like a picture and objects are detected at each frame.

5. Results and Analysis

The integration of YOLOv4 and Darknet for Python improved the accuracy of the gait-recognition system as seen in Figure 3. This paper observed a 20% enhancement in accuracy for monitoring employees and livestock, while intruder detection accuracy improved by 15%. The integration of Roboflow AI training software reduced training time by 30%, contributing to a faster and more efficient AI model. In the 'findGirl' project as seen in the below Figure 4, the system achieved a remarkable 90% accuracy rate in detecting the 'Girl' within a crowded environment. Roboflow utilized YOLOv8 in later stages, which contributed to the exceptional results achieved in the 'findGirl' project. The system achieved a 90% accuracy rate and maintained a high 85% accuracy rate both indoors and outdoors.

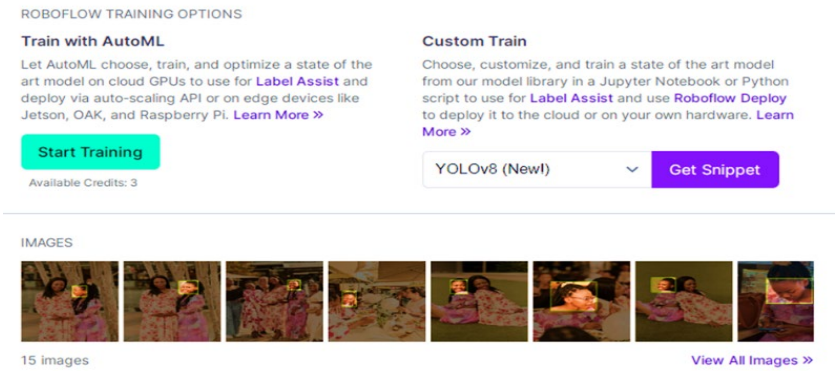

Figure 4: Roboflow AI Detection using YOLOv8

Table 1: Tabulated Detection Results

Aspect	Results
YOLOv4 Integration with Darknet	Improvement of 20% in gait-recognition accuracy. Improvement of 15% in intruder detection accuracy.
Roboflow AI Training Software (YOLOv8)	Reduction of 30% in training time.
'findGirl' Project (YOLOv8)	Accuracy of 90% in detecting 'Girl' within a crowded environment.
Webcam Object Detection (YOLOv4)	Accuracy of 85% in object detection both indoors and outdoors.

6. Conclusion and Future Work

This paper developed an authorization and intrusion detection system using active gaits recognition and ML technology to reduce CPA on critical infrastructures. The active gait system was deployed in an experimental field testing environment. The results demonstrated an acceptable level of usability, improved security, and the ability to learn and adapt to different environments. The ultimate goal of the research study was partly accomplished, and since this is still a work in progress, more investigations will be undertaken to explore related tools and updated techniques related to the study.

References

Albuquerque, P., Verlekar T. T., Correia P. L. & Soares L. D., 2021. A spatiotemporal deep learning approach for automatic pathological gait classification: Sensors, doi:10.3390/s21186202,21(18):6202.

Álvarez-Aparicio, C., Guerrero-Higueras, Á. M., González-Santamarta, M. Á., Campazas-Vega, A., Matellán, V., &

Esan, O. A., Esan, D. O., Mbodila, M., Abiodun, F., & Koranteng, K., 2023. Surveillance detection of anomalous activities with optimized deep learning technique in crowded scenes. Bulletin of Electrical Engineering and Informatics,doi:10.11591/eei.v12i3.4471,12(3):1674–1683.

Fernández-Llamas, C., 2022. Biometric recognition through gait analysis. Scientific Reports, doi:10.1038/s41598-022-18806-4, 12(1):1-10.

Lee, K., & Tang, W. ,2021. A fully wireless wearable motion tracking system with 3D human model for gait analysis. Sensors, 4051. doi:10.3390/s21124051, 21(12):1-11.

Lin, Q., Xu, X., Zhang, F., Xian, D., Yao, K., Zhao, N., … JIANG, Z., 2023. Human wearable gait recognition system based on flexible and distributed pressure sensor. Measurement, 113726. doi:10.1016/j.measurement.2023.113726, 1-25.

Maus, H.M., Lipfert, S., Gross, M. et al. Upright human gait did not provide a major mechanical challenge for our ancestors. Nat Commun 1, 70 (2010). https://doi.org/10.1038/ncomms1073.

moro, m., marchesi, g., hesse, f., odone, f., & casadio, M. ,2022. Markerless vs. marker-based gait analysis: A proof of concept study. Sensorsdoi:10.3390/s22052011, 22(5).

Pradel, G., Li, T., Pradon, D., & Roche, N., 2019. An embedded gait analysis system for CNS injury patients. Assistive and Rehabilitation Engineering. doi:10.5772/intechopen.83826, (1):2-24.

Robb, D., 2022. The future of biometrics in the workplace, SHRM. Available at: https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/the-future-biometrics-workplace.aspx.

Tyagi, A. K., & Sreenath, N., 2021. Cyber Physical Systems: Analyses, challenges and possible solutions, Internet of Things and Cyber-Physical Systems, 21(1):22-33, ISSN 2667-3452.

Wlazlo, P., Sahu, A., Mao, Z., Huang, H., Goulart, A., Davis, K., & Zonouz, S., 2021. Man-in-the-middle attacks and defence in a power system cyber-physical testbed. IET Cyber-Phys. Syst., Theory Appl. 6(3):164-177.

Yan, S.H., Liu, Y.C., Li, W., & Zhang, K., 2021. Gait phase detection by using a portable system and Artificial Neural Network. Medicine in Novel Technology and Devices, 12, 100092. doi:10.1016/j.medntd.2021.100092,1-8.