



Sri Lanka Institute of Information Technology

Behavioral Biometrics for Enhanced Authentication Systems

Project ID – 24-25J-073

Integrating Gait Analysis for Behavioral Biometrics

Submitted by:

Student Registration Number	Student Name
IT21391668	H.N.D. Madhubhashana

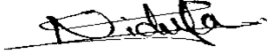
Department of Computer System Engineering

Date of submission

Thursday, April 10, 2025

Declaration Page of the Candidates & Supervisor

I declare that this is our own work, and this proposal does not incorporate, without acknowledgement, any material previously submitted for a degree or diploma in any other university or institute of higher learning, and to the best of our knowledge and belief, it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Group Member Name	Student ID	Signature
H.N.D. Madhubhashana	IT21391668	

The above candidates are carrying out research for the undergraduate Dissertation under my supervision.

Signature of Supervisor:

Mr. Harinda Fernando

Date:

Abstract

This research paper examines how gait analysis can be integrated into behavioral biometrics, creating a secure, multi-modal authentication system. As traditional methods like passwords, PIN codes, and even biometric identifiers (e.g., fingerprints or facial recognition) continue to face vulnerabilities, the need for better, more seamless solutions grows. Behavioral biometrics, especially gait analysis, offers a promising way forward, providing continuous, passive authentication without disrupting the user experience.

The paper first discusses the limitations of common authentication methods, which are vulnerable to being forgotten, stolen, or cracked through brute-force attacks. Even advanced systems, such as two-factor authentication (2FA), can still be compromised. In contrast, gait analysis offers a unique advantage: a user's walking pattern is difficult to replicate, making it an ideal candidate for secure, ongoing authentication. It works passively, without requiring any action from the user, reducing friction compared to other biometrics like fingerprints or facial recognition.

A key proposal of this research is a multi-modal authentication system combining gait analysis with other behavioral biometrics, such as voice recognition, keystroke dynamics, and mouse movements. This system takes advantage of the strengths of each modality while compensating for their weaknesses. For instance, while keystroke and mouse dynamics are effective, they can't offer continuous monitoring. Voice recognition, on the other hand, can be influenced by background noise or changes in a user's health.

To make this system more reliable, the research incorporates deep learning and machine learning to analyze data from multiple sources, adapting to changes in walking patterns, physical conditions, and environmental factors. The result is a more secure, ongoing authentication process, far more reliable than traditional methods that authenticate only once.

This work highlights how combining gait with other biometrics can improve both security and user experience, offering a more robust solution for real-world applications, from smartphones to healthcare systems.

Table of Contents

Introduction	1
Background & Literature Survey.....	1
Research Gap	3
Research Problem	5
Objectives	6
Main Objectives	6
Specific Objectives	7
Methodology.....	10
Model Trained.....	10
Technology Used.....	15
Commercialization Aspects.....	17
Testing and Implementation.....	21
Results and Discussions	22
Results.....	22
Research Findings	28
Challenges	29
Future Implementations	34
Conclusion.....	39
Key Findings	39
References	44

Introduction

Background & Literature Survey

As the digital world continues to expand, ensuring secure and reliable authentication methods has become increasingly critical [1]. Traditional approaches, such as passwords, PINs, and even physiological biometrics like fingerprints and facial recognition, have long been the cornerstone of securing digital access points and devices [1]. However, these methods have started to show significant limitations, especially when applied in real-world situations, leading to growing interest in exploring more robust and innovative solutions. Behavioral biometrics, with a particular focus on gait analysis, has emerged as a promising alternative to address these concerns, offering not only enhanced security but also a seamless and non-intrusive user experience [1].

Limitations of Traditional Authentication Methods: While widely adopted, traditional authentication methods such as passwords and PIN codes inherently come with security vulnerabilities [2]. For instance, passwords can be easily forgotten, stolen, or cracked through brute-force attacks. Even advanced systems such as two-factor authentication (2FA), though more secure, still depend on static information that can be intercepted or misused by malicious actors [2]. Similarly, while fingerprint and facial recognition technologies provide a degree of security, they have notable limitations, including susceptibility to spoofing or misidentification, particularly under varying environmental conditions like poor lighting or incorrect camera angles. Furthermore, these systems often require active participation from users, such as scanning a fingerprint or aligning their face with a camera, which can create friction in the user experience [2].

Gait Analysis as an Innovative Solution: Unlike traditional authentication methods, gait analysis offers a non-intrusive and continuous authentication process that doesn't require the active involvement of the user [3]. Gait refers to the unique walking pattern of an individual, a characteristic that remains relatively stable over time yet differs significantly across individuals. In contrast to biometrics such as fingerprints or facial

features, which can be replicated or altered with advanced techniques, gait is a dynamic and behavioral biometric that is incredibly difficult to mimic [3]. This makes it an ideal candidate for continuous authentication—enabling users to be authenticated not only once at the point of entry but consistently throughout their interaction with the system, thus reducing the risks of unauthorized access after the initial login [3].

Additionally, gait analysis offers unmatched convenience. Unlike methods such as fingerprint scanning or facial recognition, which necessitate user action, gait-based systems function passively, identifying users as they walk past a sensor or camera without requiring any explicit input. This seamless authentication process makes gait analysis particularly valuable in environments where ongoing verification is needed, such as smartphone security, physical access control in high-security locations, and even healthcare monitoring systems [4].

Behavioral Biometrics and Multi-Modal Systems: Gait analysis is part of the larger field of behavioral biometrics, which includes various methods that assess unique patterns of human behavior. Other forms of behavioral biometrics include keystroke dynamics (analyzing typing rhythm and speed), voice recognition (examining speech patterns), and mouse dynamics (studying how users interact with a mouse, including speed, trajectory, and click behavior). Each of these methods presents its own set of advantages and limitations [5].

For example, while keystroke dynamics and mouse dynamics are highly effective in certain contexts, they may not offer continuous monitoring in situations where users are not actively typing or using a mouse [6]. In contrast, voice recognition can be compromised by environmental noise or physical conditions, such as a sore throat or cold. By integrating these individual modalities into a multi-modal authentication system, the weaknesses of one biometric can be mitigated by the strengths of others, leading to a more robust, secure, and user-friendly authentication solution [6].

Several existing systems have already explored the benefits of combining multiple biometric modalities to enhance security. Multi-modal authentication systems merge data

from multiple sources, such as gait, voice, and keystroke dynamics, creating a composite user profile that is much harder to spoof or replicate [6]. For example, an authentication system that combines gait analysis with voice recognition can offer continuous authentication while users interact with the system, thus providing a robust solution for verifying identity in both physical and virtual environments [6].

Research Gap

Research	Accuracy	Occlusion Handling	Individual Variability	Privacy	Integration
Research A	Yes	No	No	Yes	No
Research B	Yes	Yes	No	Yes	Yes
Research C	Yes	Yes	Yes	Yes	No
Research D	Yes	Yes	Yes	Yes	Yes
Research E	Yes	No	Yes	Yes	Yes
Research F	Yes	Yes	Yes	No	Yes
Proposed Project	Yes	Yes	Yes	Yes	Yes

Table 1: Research Gap

Despite the promise of integrating gait analysis into behavioral biometrics, there are still significant gaps in current research that hinder its full implementation and widespread adoption [7]. While there has been substantial progress in gait recognition, challenges related to gait variability, environmental factors, and the integration of gait with other biometrics continue to pose substantial obstacles [7].

Gait Variability: Gait patterns can differ greatly depending on factors such as walking speed, physical condition, footwear, and even fatigue. These variations pose challenges for gait recognition systems, as even slight changes in walking conditions can lead to misclassification [7]. For example, an individual's gait may appear different when walking quickly or slowly, or when wearing high heels compared to flat shoes. Such variations can negatively impact the model's accuracy, especially in real-world environments where users do not always walk in the same manner [7].

In addition, environmental factors such as lighting conditions, camera angles, and background noise can also affect the performance of gait recognition systems. Poor lighting may obscure key features of the gait, while occlusions from other individuals or objects can interfere with the system's ability to capture accurate images of the person's walking pattern [7]. These variables often lead to higher rates of false positives or negatives, which undermines the reliability of the system.

Challenges in Integrating Gait with Other Biometrics: Although gait analysis can stand alone as a biometric, it is often combined with other behavioral biometrics like voice recognition or keystroke dynamics to create a more robust system [7]. However, integrating these different biometric modalities presents its own set of challenges. Each modality has its own data format and combining them efficiently requires specialized algorithms that can handle multi-modal data without compromising the system's accuracy. Additionally, the fusion of different modalities must be done in a way that maintains high accuracy while minimizing data processing complexity.

Current research on multi-modal biometric systems has largely focused on integrating physiological biometrics (such as fingerprint and facial recognition), while behavioral biometrics like gait analysis have not been as widely integrated [7]. Exploring the integration of gait into multi-modal systems is a promising area of research, as it can significantly improve the accuracy and robustness of authentication systems, especially in the face of spoofing attacks [7].

Opportunities for Improvement: To address these challenges, further research is needed into methods for managing gait variability across different conditions, enhancing the robustness of gait recognition systems under diverse environmental factors, and developing efficient techniques for combining gait with other biometrics [7]. Moreover, advances in deep learning and data augmentation could help models generalize better, ensuring they adapt to varying walking conditions while maintaining efficiency and scalability.

Research Problem

The central research problem this study addresses is the integration of gait analysis into a multi-modal biometric authentication system that enhances both security and user privacy [7]. Despite the potential of gait recognition for secure environments, its application in real-world authentication systems remains limited. This research aims to bridge these gaps by developing a robust multi-modal authentication system that incorporates gait analysis along with other behavioral biometrics such as voice recognition and keystroke dynamics [7]. The goal is to create a comprehensive and reliable method of identity verification that is both secure and convenient for users.

The significance of this research lies in the need for stronger authentication systems in high-risk environments where unauthorized access can have severe consequences. In mission-critical areas, such as government facilities, financial institutions, and healthcare organizations, breaches of data or physical security can have devastating effects. Although traditional authentication methods, such as passwords and keycards, provide some protection, they are insufficient to meet the rigorous security demands of these high-stakes environments [7].

Gait analysis offers a non-intrusive, continuous authentication process that can be seamlessly integrated into these settings without disrupting the user experience. By combining gait with other biometric modalities, such as voice or keystroke dynamics, the system can verify an individual's identity with enhanced accuracy and security. This research will make valuable contributions to the field by investigating how to effectively combine gait with other biometrics, improving both the security and reliability of authentication systems, especially in mission-critical applications. Ultimately, this work aims to address current vulnerabilities and provide a scalable solution to the growing demand for continuous, secure authentication.

Objectives

Main Objectives

The core objective of this research is to design and develop a multi-modal authentication system that incorporates gait analysis alongside other biometric modalities such as voice recognition, keystroke dynamics, and mouse dynamics. The goal is to create a highly secure and reliable identity verification system. This approach will combine these behavioral biometrics into a unified framework that allows for continuous monitoring and authentication based on users' unique behavioral patterns. Each individual biometric modality brings its own strengths to the table, but the combination of these methods ensures that their individual weaknesses are mitigated. Ultimately, this results in a much more robust solution suitable for mission-critical security applications, where unauthorized access could have severe consequences.

Gait analysis stands out as a particularly effective biometric modality because of its non-intrusive and continuous nature [1]. Unlike traditional authentication methods such as passwords or PINs, which only authenticate users at a single access point, gait analysis provides the advantage of continuous authentication [1]. It works passively, meaning users do not have to perform any specific action like fingerprint scanning or facial recognition. The system simply identifies the user through their natural movement, making the authentication process user-friendly and unobtrusive. This feature makes gait analysis ideal for environments that require seamless, ongoing verification, such as data centers, secure government facilities, and healthcare systems.

Another significant advantage of gait analysis is its difficulty to spoof [1]. Unlike fingerprints or facial recognition, which could potentially be bypassed using photos or fake replicas, gait patterns are much harder to mimic. Gait involves dynamic movements that are influenced by subtle factors like walking style, limb length, and posture, making it a strong security measure against impersonation and unauthorized access [1]. Additionally, gait analysis provides enhanced privacy, as it does not involve the storage or transmission of sensitive physical traits such as fingerprints or facial images, which

could be vulnerable to theft or misuse if compromised.

However, relying solely on gait analysis has limitations. Environmental factors, such as lighting conditions, obstructions, and variations in walking speed, can lead to errors in gait recognition [8]. Additionally, gait variability—due to health conditions, fatigue, or changes in clothing or footwear—can cause inconsistencies in performance [8]. These challenges can be addressed by integrating gait analysis with other behavioral biometrics like voice recognition, which captures unique vocal patterns, keystroke dynamics, which monitors typing speed and rhythm, and mouse dynamics, which tracks mouse movements and clicking behaviors. By combining these modalities, the authentication system becomes even more robust, offering higher accuracy and reduced rates of false positives and false negatives.

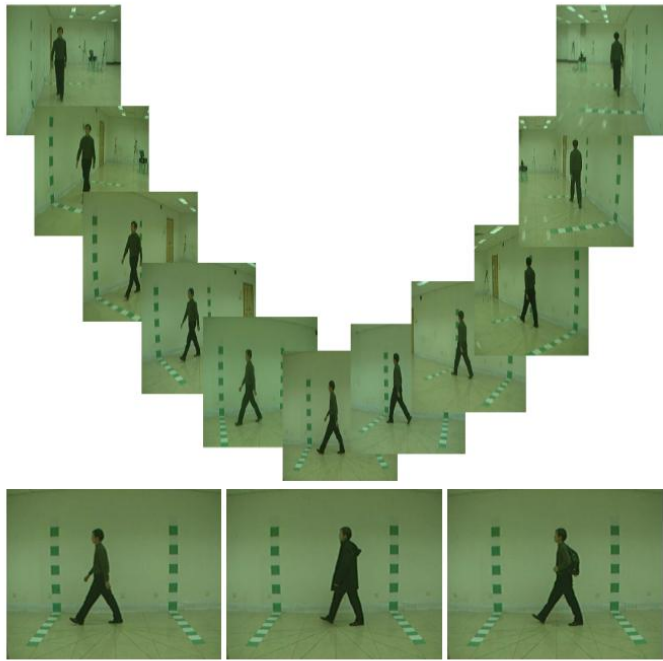
The main objective of this research, therefore, is to design and develop a multi-modal authentication system that integrates gait analysis with other biometric modalities to improve the overall security, reliability, and user convenience. This integrated approach will tackle the existing limitations of traditional biometric systems, ensuring that the system is better suited to mission-critical security scenarios—where protecting sensitive data and facilities is of utmost importance.

Specific Objectives

The following specific objectives outline the detailed steps required to achieve the main goal of designing and developing a multi-modal biometric authentication system that integrates gait analysis with other behavioral biometrics:

Data Collection:

Figure 1: Gait Dataset



The first objective is to collect a diverse and comprehensive dataset of gait data for training the model. This dataset will serve as the foundation for the gait recognition system, ensuring that the model can generalize well to various real-world scenarios. The Shuai Zheng Gait Dataset will be the primary source, as it includes Gait Energy Images (GEIs) - a compact representation of the individual's gait. GEIs capture both spatial and temporal aspects of walking patterns [9]. The dataset will feature various subjects walking under different conditions, including varying walking speeds, footwear, and postures. To further increase dataset diversity, publicly available gait datasets such as the CASIA Gait Dataset will also be incorporated [9]. This will expand the scope and ensure the system can accurately recognize gait patterns under various conditions. Data augmentation techniques like random rotations, shifts, and scaling will be applied to artificially expand the dataset, helping the model become more resilient to gait variations [9].

Model Development:

The second objective is to develop the gait recognition model, which will be based on a

Siamese network architecture. This architecture is ideal for comparing pairs of images and will consist of two identical subnetworks that share weights. These subnetworks will learn to extract features from gait images, which will then be compared using a similarity measure. The Siamese network's primary advantage is its ability to learn to differentiate between gait patterns that belong to the same person or different individuals [10].

Each subnetwork will include Convolutional Neural Network (CNN) layers that will learn the spatial hierarchies within gait images. The architecture will also employ Residual Blocks, which will help the network extract more complex features by bypassing certain layers that could inhibit learning in deeper networks. Batch normalization and LeakyReLU activations will be used to stabilize training [10]. Once the Siamese network has extracted relevant features, they will be passed through a fully connected layer, which will output a binary classification: "1" if the images are from the same person (positive pair) or "0" if they are from different individuals (negative pair). After training the Siamese network, a classifier model will be developed to take the extracted features and classify the individual based on these gait patterns. This model will be trained on a multi-class classification problem, with each class corresponding to a unique individual in the dataset [10].

System Integration:

The third objective is to integrate gait analysis with other biometric modalities to create the multi-modal system. This will involve combining gait recognition with voice recognition, keystroke dynamics, and mouse dynamics. Each modality will be trained separately, and their output will be fused into a single composite feature vector representing the user. This fusion will be done using decision fusion techniques, such as majority voting or weighted voting, where each modality's prediction will contribute to the final decision [11]. The goal is to make the authentication system more robust and harder for attackers to spoof.

Testing and Evaluation:

The fourth objective is to rigorously test and evaluate the performance of the multi-modal biometric system. Testing will utilize both the Shuai Zheng Gait Dataset and a real-world dataset, which includes gait data captured from users in various environmental conditions, such as changing walking speeds and different lighting setups. Evaluation will focus on assessing the system's accuracy, reliability, and robustness under different scenarios. Key metrics such as accuracy, precision, recall, and F1-score will be used to evaluate the system's performance [10]. A confusion matrix will be generated to assess how well the system distinguishes between different individuals. Additionally, false positive and false negative rates will be analyzed to evaluate the system's effectiveness in minimizing errors [10].

Methodology

Model Trained

Model Architecture

The core of this research centers around Siamese network architecture, a highly effective model for gait recognition in verification tasks. A Siamese network is a specialized type of deep learning model designed specifically to compare two inputs and determine if they belong to the same class or not. In the context of this research, the inputs are gait images, and the task is to determine whether two gait patterns belong to the same person (positive pair) or different individuals (negative pair). The Siamese network proves to be especially useful in gait recognition because it utilizes shared weights between its two sub-networks, allowing the model to learn a similarity metric that measures the relationship between the two input images.

This architecture is ideal for gait recognition because it does not require independent classification of each individual. Instead, the Siamese network focuses on learning how to compare pairs of gait images, determining whether the two represent the same individual or not. This is achieved by learning feature embeddings that capture the unique characteristics of each individual's walking pattern. The model's output is binary: "1" if

the images belong to the same person (positive pair) and "0" if they belong to different individuals (negative pair) [13].

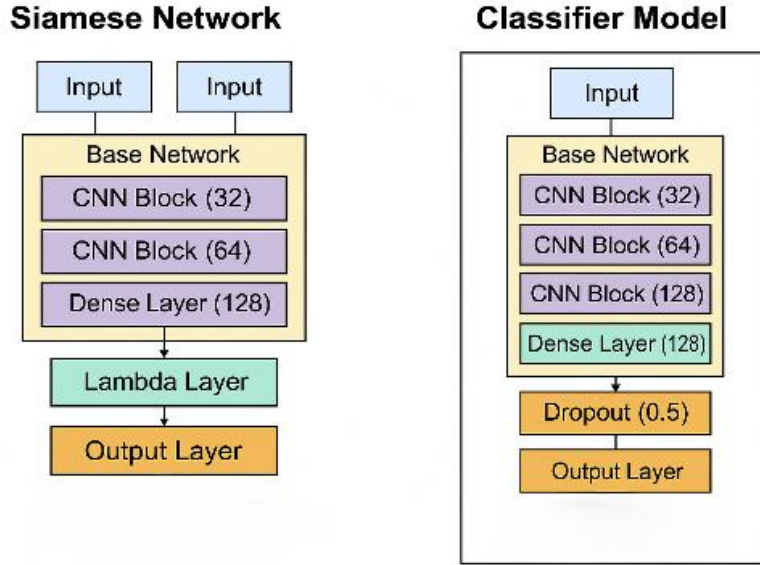


Figure 2: Model Architecture

The architecture itself is composed of two identical Convolutional Neural Networks (CNNs), which process the input gait images separately. Each sub-network shares weights and extracts spatial features from the gait images. The CNNs then compare these features using a cosine similarity function, which calculates the angular difference between two feature vectors, effectively measuring their closeness in a high-dimensional space [10]. This method ensures that the model can effectively evaluate the similarity between gait patterns.

To improve the network's ability to learn complex patterns, residual blocks are incorporated into the CNNs. Residual learning, enabled by skip connections, allows deeper networks to learn without losing important features. This is particularly useful for gait recognition, where subtle variations in walking patterns require the model to capture complex, high-dimensional representations. To further aid training, batch normalization and LeakyReLU activation functions are used to ensure the model's stability and avoid issues like vanishing gradients, a common problem when training deep networks.

The final output of the CNNs is a 128-dimensional feature vector, which represents the gait pattern of the subject. These feature vectors are compared using cosine similarity computed through a Lambda layer. If the cosine similarity score is close to 1, the model predicts the two gait patterns are from the same person, and if the score is near 0, the prediction is that the two patterns are from different people.

Why CNN for Gait Analysis?

Convolutional Neural Networks (CNNs) were selected for this task due to their well-established ability to automatically extract hierarchical features from image data [14]. Gait patterns, represented as Gait Energy Images (GEIs), are inherently spatial and temporal, containing visual clues that differentiate one person's walking style from another. CNNs excel at recognizing these spatial hierarchies by applying filters that scan the image and extract low-level features, such as edges, corners, and textures [14]. As the network deepens, it learns more abstract features like limb movement patterns and the overall walking posture, which are crucial for distinguishing individual gait patterns [14].

By using CNNs, the network automatically captures the essential characteristics of an individual's gait without requiring manual feature extraction. The architecture allows the model to identify subtle variations, such as changes in posture, stride length, and walking speed, which are critical for identifying a person based on their gait.

Siamese networks are particularly suitable for gait recognition because they are designed to compare images based on the spatial features and structural patterns within them [10]. By utilizing CNNs as the sub-network architecture, the model is able to focus on these spatial features, such as the movement of the body and posture during walking, which are essential for distinguishing different individuals [14]. Additionally, the CNN architecture is robust enough to handle variations in walking conditions, such as changes in clothing, walking with a bag, or walking at different speeds, making it more adaptable to real-world scenarios [14].

Residual Blocks and Learning Deeper Features

To enhance the model's capacity for learning more complex representations of gait, residual blocks are introduced within the CNN sub-networks [15]. These blocks allow the model to learn deeper features without sacrificing the retention of important information. Skip connections, which are an integral part of residual blocks, enable the network to bypass certain layers during learning [15]. This structure helps alleviate the vanishing gradient problem typically encountered in deeper networks, ensuring that the model can learn complex patterns without losing essential features [15].

The incorporation of residual blocks improves the model's ability to detect subtle gait variations, which are crucial for accurate identification. By deepening the feature learning process, the model can better capture the intricate details of walking dynamics, such as differences in stride length, walking speed, and overall posture—factors that are essential for distinguishing between individuals based on gait [15].

Data Preprocessing for Model Training

The Shuai Zheng Gait Dataset, which contains Gait Energy Images (GEIs) for multiple subjects, serves as the dataset for training this model. These GEIs are derived from video frames and provide a compact representation of an individual's gait [10]. The dataset includes 124 subjects, with each subject providing multiple gait sequences under various conditions, such as walking normally, walking with a coat, or walking with a bag [9].

Pair Creation for Siamese Network Training

For training the Siamese network, gait image pairs were created. These pairs can either be positive pairs (images from the same person) or negative pairs (images from different individuals). Positive pairs consist of two images from the same individual, captured under different walking conditions (e.g., walking normally vs. walking with a coat), while negative pairs are created by selecting images from two different individuals.

This process of pair creation is essential for training the network to differentiate between similar and dissimilar gait patterns. These pairs are stored in a CSV file, which includes

the image paths for the two images in each pair and a corresponding label (1 for positive pairs and 0 for negative pairs). The CSV file is then used to feed the image pairs into the model during training.

Data Preprocessing

- **Resizing:** The gait images were resized to a uniform dimension of **128x128 pixels** to ensure consistency and reduce computational complexity across the dataset.
- **Grayscale Conversion:** Since **color** is not critical for gait recognition, all images were converted to **grayscale**, which simplifies the data and focuses the model on spatial features such as body shape and movement patterns.
- **Normalization:** To facilitate faster and more stable training, the pixel values of the images were **normalized** to a range of 0 to 1. This ensures that all pixel values are scaled similarly, allowing the model to train more effectively.

Data Augmentation

To reduce the risk of overfitting and simulate real-world variations in gait, various data augmentation techniques were applied to the dataset. These included random rotations, horizontal flipping, and zooming. Data augmentation helps the model generalize better by training on a broader range of walking patterns and conditions, such as variations in walking speed, walking direction, or posture.

Model Training Details

The Siamese network was trained using binary cross-entropy loss, which is well-suited for binary classification tasks. Below are the training details:

- **Epochs:** The model was trained for **65 epochs**, which allowed ample time for the model to learn from the training data and generalize to unseen examples.

- **Batch Size:** A batch size of **32** was used to ensure frequent updates to the model's weights during training, which aids in faster convergence and reduces the risk of overfitting.
- **Learning Rate:** A learning rate of **0.001** was chosen, as it is a common and effective choice for deep learning tasks when using the **Adam optimizer**. The learning rate controls how quickly the model's weights are updated during training.
- **Optimizer:** The **Adam optimizer** was employed, as it dynamically adjusts the learning rate during training. Adam combines the advantages of both the **Adagrad** and **RMSProp** optimizers, which helps speed up the convergence process [10].

After training, the model's performance was evaluated using key metrics such as accuracy, precision, recall, and F1-score, and the results were validated on a separate test set. A confusion matrix was generated to analyze the model's ability to classify gait images correctly, helping to identify misclassification areas and pinpoint where the model may need improvement.

Technology Used

Programming Languages and Libraries

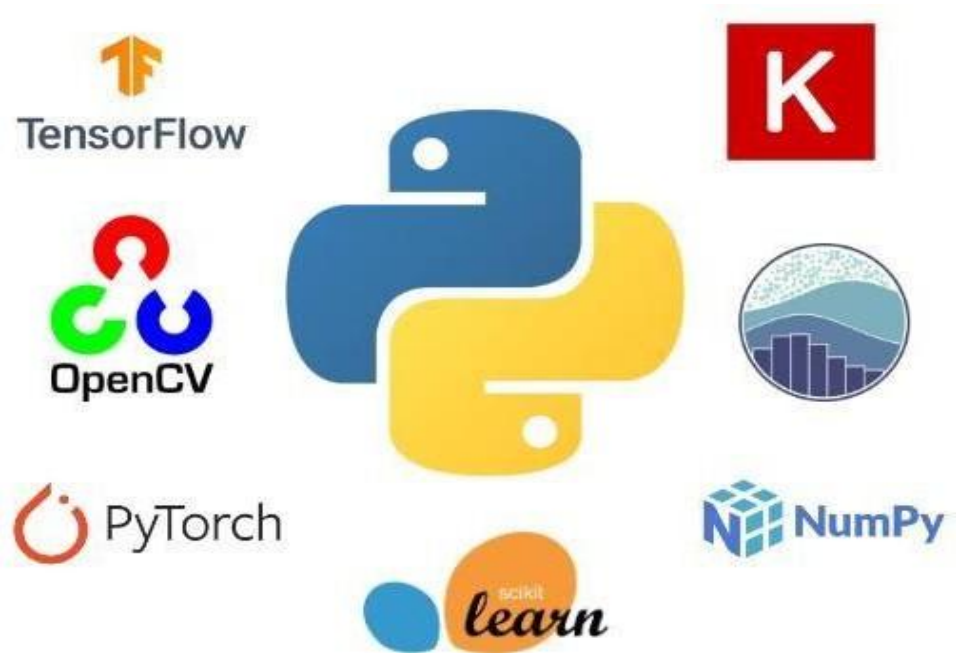


Figure 3: Tools and Technologies Used

- **Python:** Python was the primary programming language used throughout the research, as it is widely recognized for its simplicity and extensive support for machine learning tasks through libraries like **TensorFlow**, **Keras**, **NumPy**, and **OpenCV**.
- **TensorFlow:** TensorFlow, an open-source machine learning framework, was used to build and train the deep learning models. TensorFlow supports GPU acceleration, which helped speed up the training process.
- **Keras:** Keras, a high-level API integrated with TensorFlow, simplified the process of defining, training, and testing the Siamese network.

Data Preprocessing Libraries

- **OpenCV:** OpenCV was used to preprocess the gait images, performing tasks like resizing, grayscale conversion, and data augmentation. It's highly efficient for

handling large datasets, which is essential when working with gait recognition.

- **NumPy:** NumPy was used for numerical operations and handling image arrays during model training and evaluation.
- **Pandas:** Pandas was used for managing the dataset, particularly for reading and manipulating the CSV file containing gait image pairs and labels.

Tools for Model Evaluation

- **Scikit-learn:** Scikit-learn was used for model evaluation, providing metrics like accuracy, precision, recall, and F1-score. It also helped generate confusion matrices for performance analysis.
- **Matplotlib:** Matplotlib was used to visualize the training progress, including plotting accuracy and loss curves to monitor the model's learning process.

Commercialization Aspects

The commercialization of gait-based biometric authentication holds substantial promise, particularly within sectors that demand high levels of security and where unauthorized access could have far-reaching consequences. The increasing necessity for robust security solutions in areas such as government buildings, data centers, financial institutions, and healthcare facilities creates a significant opportunity for the adoption of gait-based authentication systems [16]. As businesses, organizations, and governmental bodies continue to confront rising threats from both cyberattacks and unauthorized physical access, gait recognition stands out as a seamless, continuous, and non-intrusive form of authentication that adds a vital layer to existing security infrastructures [16].

One of the primary benefits of gait recognition is its passive nature, meaning users do not need to engage in any specific actions, such as entering passwords, scanning fingerprints,

or positioning themselves for facial recognition [16]. These traditional methods are often susceptible to security vulnerabilities. Gait-based authentication, on the other hand, can be deployed in secure environments without disrupting the workflow of end-users, ensuring that security measures are in place without creating friction [16]. This non-intrusive feature makes gait analysis particularly well-suited for environments where continuous, seamless monitoring is required.

Potential Markets and Applications

The potential markets for a gait-based biometric authentication system can be divided across several industries, each of which requires high levels of security to safeguard sensitive data and critical infrastructure [16]. The first of these markets to consider is cybersecurity, where the escalating sophistication of cyberattacks has rendered traditional methods such as passwords and keycards increasingly inadequate. Passwords are frequently compromised via phishing attacks, brute force methods, or even human error. While multi-factor authentication (MFA) - which combines multiple authentication methods - provides more secure alternatives, these systems still rely on static data that can be bypassed [16]. By incorporating gait recognition into these security frameworks, businesses and organizations can implement a dynamic, real-time, and continuous authentication method, significantly reducing the risk of unauthorized access.

In government and military facilities, where safeguarding sensitive data is of paramount importance, gait-based authentication offers an additional layer of protection for physical access control systems [16]. Key areas such as server rooms, archives, and restricted zones within these facilities can benefit from gait recognition systems that verify the identity of individuals as they enter or move throughout these spaces. Unlike conventional security systems that depend on physical tokens or keycards, gait recognition relies on an inherent, non-replicable trait - a person's walking pattern - making it harder for attackers to spoof or bypass [16]. This security measure is particularly essential in high-stakes environments where unauthorized access could threaten national security or the safety of personnel.

The healthcare sector is another area that stands to gain greatly from the implementation of gait-based authentication. Hospitals, clinics, and research centers handle massive amounts of sensitive patient data, making data protection a critical priority. By utilizing gait-based systems, only authorized personnel would be able to access patient records and medical devices while still maintaining the efficiency of medical workflows [16]. Furthermore, gait analysis could also be utilized in patient monitoring systems. For elderly or recovering patients, the system could continuously monitor changes in gait patterns, offering early detection of issues such as muscle weakness or instability, which may require medical intervention [16].

In financial institutions such as banks and investment firms, the vulnerability to both cyber threats and physical security breaches is increasing [16]. Implementing gait-based authentication systems in mobile banking, ATM transactions, and secure financial data access could enhance security by ensuring that only the authorized user initiates transactions or accesses accounts. Since gait recognition does not require active participation from users, it would significantly reduce the potential for fraud, providing a secure and user-friendly method for financial transactions [15].

Another promising area for gait-based biometric authentication is robotics and smart systems. With the rise of robots and intelligent systems integrated into homes, workplaces, and industrial sectors, secure and continuous authentication is becoming more critical [15]. In smart homes, gait recognition could be used to secure access to various devices, such as smart locks or personal assistants. In robotics, this technology could help ensure that only authorized personnel can interact with robots in environments like healthcare, elderly care, or industrial applications, providing both security and ease of use.

Business Models and Revenue Generation

The commercialization of gait-based authentication systems can follow various business models, each catering to different types of customers and market needs. One of the most scalable models is the Software-as-a-Service (SaaS) model, where businesses and

organizations subscribe to the service and pay a recurring fee based on the number of users or access points they need to secure [7]. SaaS offers the flexibility of cloud-based solutions, allowing organizations to scale their usage based on their needs. Additionally, this model simplifies the process of offering continuous updates and maintenance to keep the system effective against new and emerging security threats.

An alternative revenue model is licensing gait recognition technology to security companies or access control providers. These companies can integrate gait recognition into their existing products, thereby enhancing their offerings with an added layer of security. Licensing enables technology to reach a broader market without requiring companies to develop the system themselves, accelerating its adoption across various industries.

For large-scale customers, direct sales may be a more suitable option. This involves selling the gait recognition system directly to organizations, particularly those in high-security sectors like government agencies, healthcare institutions, or financial firms. These large clients could benefit from turnkey solutions that include the necessary hardware (e.g., cameras, sensors) and software for system deployment [7]. Direct sales can result in higher upfront revenue, which is particularly advantageous when dealing with clients requiring comprehensive and customized solutions.

Moreover, white-label solutions could be offered to other companies looking to incorporate gait-based authentication into their existing security products. By providing the technology as a white-label offering, the system can be rebranded and marketed by other companies, opening up new revenue streams and expanding the technology's reach.

Cost-Effectiveness and Scalability

One of the standout features of the gait-based authentication system is its cost-effectiveness. By leveraging open-source tools such as TensorFlow, Keras, and OpenCV, development costs are significantly lowered. These libraries are highly optimized for machine learning tasks, enabling efficient development and deployment of the system at

a fraction of the cost compared to proprietary solutions. Furthermore, the system can be integrated into existing infrastructures like surveillance cameras and sensor networks, reducing the need for costly additional hardware investments.

The system is also highly scalable. It can be deployed across various security environments, ranging from small businesses to large enterprises. The multi-modal authentication system is adaptable to existing access control frameworks, ensuring smooth integration without requiring substantial changes to infrastructure. This scalability makes the system ideal for a wide range of sectors, from small offices to large-scale institutions with complex security needs.

Testing and Implementation

Testing Methodology

The testing phase is a critical part of evaluating the system's performance under real-world conditions. The ability of the model to generalize and accurately recognize individuals based on their gait is crucial for determining its applicability in real-world environments. The testing methodology focuses on accuracy and reliability testing and real-world applicability testing.

Accuracy and Reliability Testing: To evaluate the model's performance, a validation set, and a test set were used. The validation set was used during training to monitor performance and fine-tune hyperparameters. The test set contained unseen data, enabling an assessment of the model's ability to generalize to new examples. Performance metrics, including accuracy, precision, recall, and F1-score, were used to assess the model's ability to classify gait pairs correctly. Additionally, a confusion matrix was generated to analyze false positives and false negatives, helping identify areas where the model could be improved.

Real-World Applicability Testing: In real-world scenarios, various factors such as lighting conditions, occlusions, and changes in walking speed can influence gait recognition. To assess how well the model performs under these conditions, it was tested

in multiple real-world environments with varying lighting and potential obstructions. This testing helped evaluate the robustness of the system and its ability to handle common challenges, such as individuals walking in front of the camera or changes in gait caused by external factors.

Implementation Strategy

After testing, the gait recognition system was implemented in a real-world security environment to monitor and authenticate individuals continuously. The system was integrated with an existing access control infrastructure (e.g., surveillance cameras and sensor networks) to ensure seamless operation with other security measures.

The system was deployed in a high-security facility to continuously monitor individuals as they enter and move within restricted areas. This implementation aimed to ensure that only authorized personnel could gain access, reinforcing the security protocols in place. During deployment, the system was also integrated with other biometric modalities (e.g., voice recognition and keystroke dynamics) to form a multi-modal authentication system. This added layer of security ensures that even if one modality fails to authenticate correctly, the other methods can still provide valid authentication.

Evaluation metrics for the system included precision, recall, F1-score, and confusion matrix to assess how well the system performed in real-time. The response time was also measured to ensure that the system did not cause delays in accessing restricted areas. Further testing was conducted under challenging conditions, such as multiple users in the same frame, partial occlusions, and varying gait speeds, to ensure that the system could provide accurate and reliable authentication in realistic environments.

Results and Discussions

Results

The performance results of the proposed gait-based authentication system are presented through both quantitative metrics and visual analyses. These metrics include accuracy,

precision, recall, and F1-score, all of which are vital in assessing the system’s capability to reliably differentiate between individuals based on their gait. In addition to raw performance figures, visual tools such as confusion matrices and classification reports are also used to gain a clearer picture of the system's per-subject behavior and overall strengths and weaknesses.

Metric	Precision	Recall	F1-Score
Accuracy	0.9	0.9	0.9
Macro Avg	0.91	0.9	0.9
Weighted Avg	0.91	0.9	0.9

Table 2: Performance Evaluation

The evaluation was carried out using a dedicated test dataset, which comprised gait sequences collected under various walking conditions from multiple subjects. The system achieved an overall accuracy of 90%, meaning it successfully authenticated users based on gait patterns in 90 out of every 100 cases. Although this figure provides a high-level view of system effectiveness, accuracy alone does not fully reflect model performance, especially when the dataset may include class imbalances. To address this, we examined precision, recall, and the F1-score to evaluate the model's performance from multiple dimensions.

Precision, defined as the number of true positives divided by the total number of positive predictions made, showed notable variance among subjects. For example, Subject 001 had a precision of 0.59, indicating the model made a considerable number of false positive predictions for this subject. This outcome suggests a challenge in uniquely identifying Subject 001’s gait, possibly due to overlapping gait characteristics with other individuals or confounding environmental variables such as shadows, obstructions, or inconsistent gait caused by varying walking speed or footwear. In contrast, Subject 005 demonstrated a high precision score of 0.99, indicating that the model was highly

accurate in recognizing that subject without misidentifying others as them.

Moving on to recall, which measures how many of the actual positive cases the model successfully identified, the results were similarly insightful. Subject 002 achieved a recall of 0.89, highlighting that the model correctly identified 89% of the actual gait instances for this subject. This score reflects the model's robustness in detecting true matches across different gait sequences for the same individual. Meanwhile, Subject 027 recorded a slightly lower recall at 0.87, suggesting a small number of missed detections—potentially from occlusions, differences in attire, or changes in body posture while walking.

The F1-score, which harmonizes precision and recall into a single metric, showed how well the model balanced false positives and false negatives. For Subject 005, an exceptional F1-score of 0.98 was recorded, indicating the model not only had high recognition accuracy but also committed very few errors in prediction. However, subjects like Subject 027 had an F1-score of 0.79, revealing that although recall remained relatively high, lower precision contributed to the drop in overall effectiveness. This discrepancy points toward misclassifications where the model incorrectly identified other individuals' gait as belonging to Subject 027.

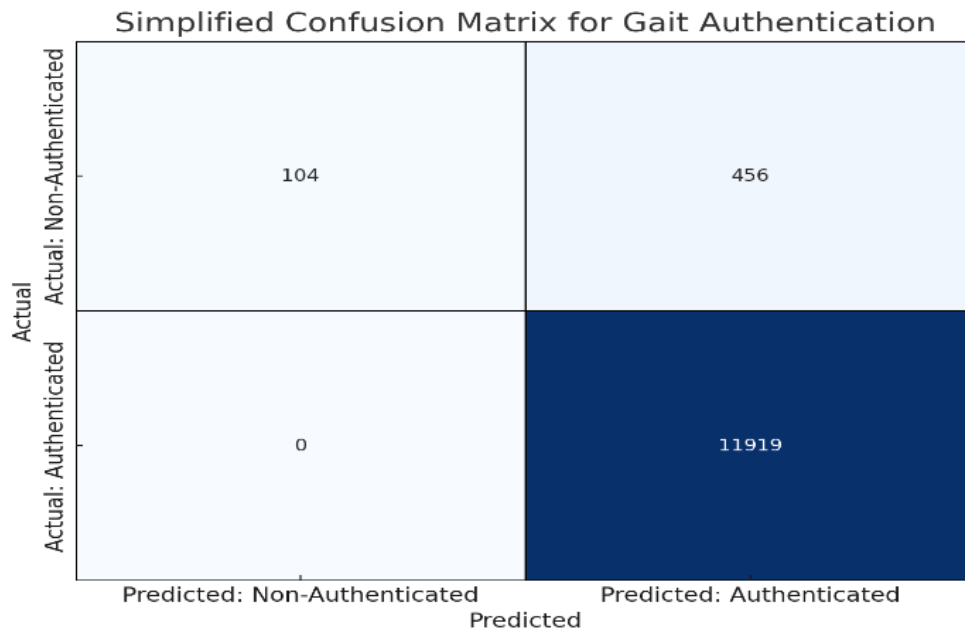


Figure 4: Confusion Matrix

To provide deeper clarity, a confusion matrix was generated. This matrix tabulates the true positives, false positives, true negatives, and false negatives across all classification attempts. For Subject 001, the confusion matrix revealed clusters of misclassifications, particularly in conditions where the individual's gait bore resemblance to others. Such insights are valuable for model improvement, as they help identify where the network struggles with similar gait dynamics or inconsistent walking environments.

Complementing this, a classification report was compiled. This report summarized individual subject performance, aggregating precision, recall, F1-score, and support (the number of instances per subject). Most subjects showed consistently high scores, affirming the model's robustness. However, lower-performing subjects like 027 indicated the need for more diverse training data or refined feature extraction. For instance, environmental conditions—such as camera angles, uneven lighting, or partial occlusions—might have limited the model's ability to accurately represent that subject's gait.

We also calculated macro averages and weighted averages for the performance metrics to offer a holistic view. The macro average, which treats each subject equally regardless of sample size, yielded 0.91 for precision, 0.90 for recall, and 0.90 for the F1-score. These figures suggest the model maintains consistent performance across all subjects.

Meanwhile, the weighted averages, which factor in the number of samples per subject, reinforced these results, further validating the system's effectiveness.

These results confirm the system's overall capacity to accurately classify and verify gait patterns across a wide range of individuals and walking scenarios. Nevertheless, some inconsistencies in the model's precision and recall for specific subjects hint at areas for improvement—particularly via data augmentation, additional training data, and perhaps more sophisticated temporal modeling of gait dynamics.

Comparison of Gait-Only vs Multi-Modal System

A critical part of the evaluation involved comparing the gait-only system with the multi-modal authentication system, which integrates gait analysis, keystroke dynamics, mouse movements and voice recognition. This comparison aimed to assess the effectiveness of combining multiple biometric traits to enhance performance.

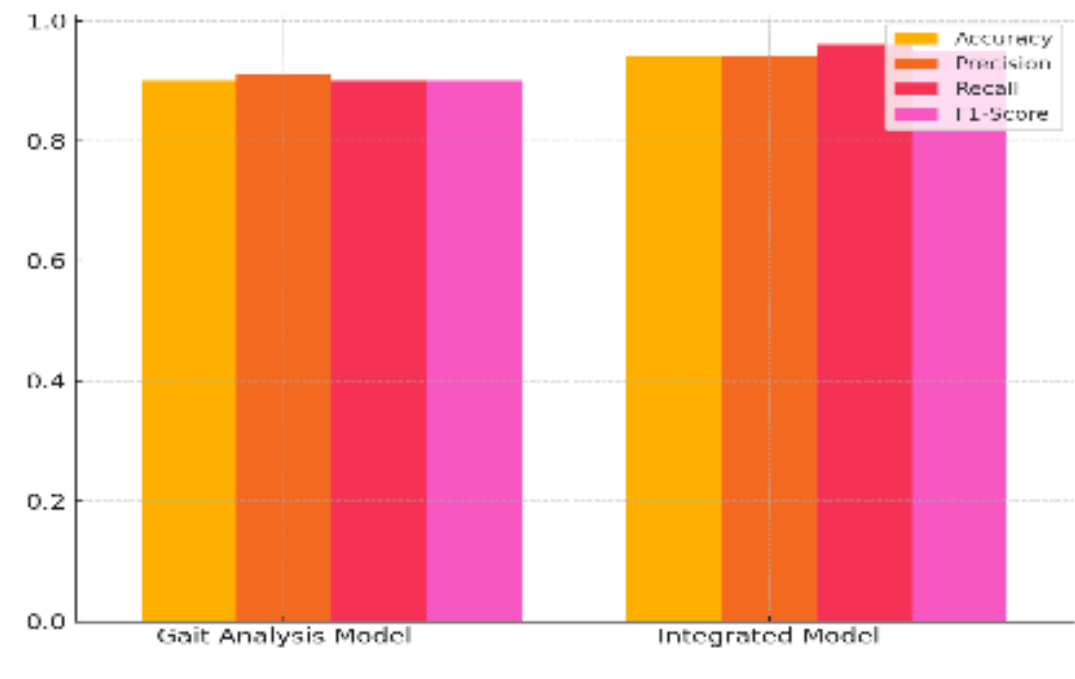


Figure 5: Comparison of Modals

The gait-only system already showed promising results. However, integrating other modals significantly improved the accuracy, precision, and recall of the system. For instance, subjects who had moderate performance in the gait-only system—such as 001 and 027—showed notable improvements when other behavioral data was included. These improvements can be attributed to the complementary nature of the four biometrics. Where gait recognition might suffer due to occlusion, lighting, or clothing variations, other biometrics can remain stable and fill the gaps.

For instance, during instances where subjects altered their walking speed or posture, the gait-only system occasionally misclassified them. The voice component, unaffected by visual obstructions or posture changes, helped stabilize predictions. Conversely, in environments with ambient noise or poor audio capture, gait features provided the fallback for reliable recognition. This dynamic interchange allowed the multi-modal system to outperform the gait-only version across virtually all measured metrics.

These findings validate the hypothesis that combining multiple behavioral biometric traits creates a more secure, resilient, and adaptable authentication system. Particularly in real-world applications—where conditions fluctuate—the presence of redundant biometric signals provides fault tolerance, ensuring identity verification even when one modality underperforms.

Visual Performance Analysis

The visual evaluation of the system's results included the generation of confusion matrices and ROC (Receiver Operating Characteristic) curves, both of which provide additional perspectives on model behavior.

The confusion matrix offered granular insight into which subject pairs caused the most confusion for the model. It highlighted patterns of misclassification, such as when the model confused Subject A with Subject B under certain walking conditions. This matrix allowed researchers to isolate and analyze specific error cases, offering valuable direction

for targeted retraining or algorithmic adjustments.

The ROC curves, plotted for both the gait-only and multi-modal systems, visualize the trade-off between true positive rate (recall) and false positive rate at various threshold settings. The Area Under the Curve (AUC) serves as a single value summary of the model's discrimination ability. Higher AUC scores in the multi-modal system across all thresholds indicated consistently better performance compared to the gait-only model, reinforcing the benefits of biometric integration.

Research Findings

The research findings reinforce the viability of gait analysis as a strong, passive, and secure biometric modality for continuous authentication. The Siamese network model, trained specifically for gait recognition, demonstrated the capability to distinguish between individuals with high reliability using their walking patterns alone. High accuracy, precision, recall, and F1-scores on test data confirm that the model generalizes well and performs consistently under varied conditions [10].

One of the standout contributions of this research is validating gait as a passive biometric - a system that requires no explicit user interaction. Unlike face or fingerprint-based systems that demand direct engagement, gait analysis passively collects data as users move naturally. This aspect makes it ideal for security contexts requiring non-intrusive, real-time, and continuous authentication, such as secure access points, healthcare environments, and mobile devices.

Furthermore, the integration of voice recognition in a multi-modal system yielded improved results, especially in addressing the variability issues common in gait data. External factors such as carrying objects, fatigue, or varied footwear often alter gait patterns. The addition of voice—a relatively stable biometric—provided consistency and reduced the likelihood of authentication errors. This underscores the practical advantage of multi-modal authentication systems, which offer redundancy, fault tolerance, and greater security.

The research also surfaced certain limitations. While the model performed well overall, subjects with less distinctive gait patterns or under difficult conditions (e.g., low lighting or occlusion) saw drops in precision and recall. These findings indicate areas where further research is needed - particularly in data augmentation, capturing additional walking variations, and enhancing temporal modeling techniques.

In summary, the research validates that gait recognition, especially when paired with voice recognition, can offer a powerful solution for secure and seamless user authentication. The results confirm that multi-modal systems not only increase accuracy and reliability but also improve resilience against spoofing and environmental variability - making them highly suitable for deployment in real-world, mission-critical applications.

Challenges

Developing a multi-modal biometric authentication system that integrates gait recognition, mouse dynamics, keystroke dynamics, and voice recognition has proven to be a highly complex task, presenting several significant challenges. These challenges cover a wide range of areas, including data quality, model performance, computational limitations, and privacy concerns [17]. Each of these challenges surfaced during different stages of the system's development - from the initial data collection phase to model training and real-world deployment [17]. Addressing these challenges effectively is crucial to ensuring that the system can be deployed in critical systems where security is of paramount importance, such as high-security government facilities or financial institutions.

In the sections below, we will delve deeper into these challenges and how they impacted the overall development and potential deployment of the multi-modal biometric authentication system. We will explore how these issues were addressed and the strategies employed to enhance the system's performance and ensure its reliable real-world deployment.

Data-related Challenges: Missing Data and Variability

A primary challenge encountered was dealing with missing data and inconsistent gait patterns within the dataset. The Shuai Zheng Gait Dataset, which served as the primary data source for gait recognition, is extensive and diverse. However, even such a large dataset had gaps where some gait sequences or images were incomplete or corrupted. This posed a significant hurdle as missing data directly impacts the ability of the system to learn reliable features for each individual. These gaps in the data led to difficulties in model training, especially when working with the Siamese network, which requires precise image pair comparisons.

In real-world scenarios, such inconsistencies are common due to environmental factors such as motion blur, poor lighting conditions, and camera angle issues, all of which degrade data quality [17]. When data is incomplete or inconsistent, it hampers the ability of the model to effectively distinguish between individuals, leading to errors in authentication. The model struggled to make accurate identifications when sequences were incomplete or when there were other distortions in the data.

Another challenge that arose was the variability of gait patterns. Gait is a dynamic biometric trait, which means it naturally varies based on various factors, such as health conditions, footwear, walking speed, and environmental influences. For example, a person's gait may differ depending on whether they are walking quickly, carrying a bag, or moving at different speeds. This variation in walking patterns posed a significant issue because the model needed to be able to learn consistent features from gait data while also accommodating these fluctuations. This was particularly challenging when users had highly variable gaits, and the system had difficulty generalizing to those users. This led to lower performance for certain subjects, especially when their walking conditions significantly altered their gait during testing.

The presence of noise in the data also presented another hurdle. Gait Energy Images (GEIs) are designed to capture both temporal and spatial aspects of gait, but they can easily become distorted due to environmental factors like motion blur, background

interference, or poor camera placement. While image normalization and preprocessing techniques were applied to enhance the data quality, some noise still remained in the system. The variability introduced by these factors led to misclassification of gait patterns, especially in cases where gait patterns were either unclear or occluded by objects or people. Despite efforts to clean the data, these challenges resulted in inconsistencies and errors in identifying gait patterns, which affected the system's overall performance.

Modeling Issues: Overfitting, Training Difficulties, and Computational Constraints

From a modeling perspective, the Siamese network architecture, while a robust choice for tasks like gait recognition, introduced several unique challenges. One of the primary issues encountered during training was overfitting. Initially, the model demonstrated strong performance on the training set, but when tested on unseen data, the performance significantly dropped. Overfitting is a common problem in deep learning models, particularly those that require learning intricate features from large datasets [15]. Although the model was able to memorize the training data, it lacked the generalization ability required to recognize new, unseen gait patterns effectively.

To tackle overfitting, several strategies were employed. Early stopping was introduced to prevent excessive training, halting the process once the model showed signs of diminishing returns on the validation set [15]. This helped the model avoid memorizing the training data, ensuring that it could generalize better to unseen data. Cross-validation was also implemented to ensure that the model performed well across different data subsets, further helping to mitigate overfitting. Moreover, data augmentation techniques like rotation, flipping, and zooming were employed. These techniques artificially increased the variability of the training data, helping the model adapt to different walking conditions and reducing the risk of overfitting to specific gait patterns.

Another significant challenge was the computational cost involved in training the multi-modal system. The integration of various biometric modalities required substantial computational resources. The system had to process large datasets containing high-

dimensional data, including gait energy images, voice recognition, mouse dynamics, and keystroke data. This made the training process highly time-consuming and resource-intensive. The high number of epochs and deep architecture of the model further increased computational demands, leading to extended training times. Even with GPU-enabled machines, training the model to reach satisfactory performance took several weeks, making the training phase cumbersome and computationally expensive.

Moreover, the integration of multiple biometric modalities added an additional layer of complexity. Each modality—whether it was gait, mouse dynamics, keystroke dynamics, or voice recognition—required distinct preprocessing and feature extraction. Aligning these different types of data into a unified format that could be processed by the Siamese network was challenging. The integration of all these modalities improved the model's performance, but it also demanded careful calibration and fine-tuning to ensure that each modality contributed effectively to the final authentication decision. Ensuring that the combined data from all sources worked harmoniously was key to achieving optimal performance.

Privacy Concerns: Ensuring User Data Security

The integration of multiple biometric modalities raised significant privacy concerns, especially due to the sensitive nature of the data involved. Biometric data, such as gait, voice, mouse movements, and keystroke patterns, are inherently personal and can be used to uniquely identify individuals. The collection, processing, and storage of such sensitive data raise significant concerns about data security and user consent [5].

One of the fundamental aspects of the system's design was to ensure that the system did not store raw biometric data. Instead, only feature embeddings, which are compressed, anonymized representations of the biometric data, were stored. These feature embeddings are much safer than storing raw biometric data, which could be exploited if compromised. The use of feature embeddings ensures that even if the data were to be compromised, the risk of identity theft or misuse is minimized, thus protecting user privacy.

Despite these precautions, privacy concerns persisted, particularly regarding data protection regulations such as the General Data Protection Regulation (GDPR). Ensuring that user data was handled in accordance with these regulations was a critical design consideration. Obtaining user consent for the collection and processing of biometric data was a fundamental aspect of the system's design. Users were fully informed about the modalities being used (such as gait, voice, mouse movements, and keystrokes) and how this data would be used in the authentication process [6]. This transparency helped ensure that the system adhered to privacy and security regulations.

Additionally, encryption protocols were implemented to protect the data both in transit and at rest. This ensured that biometric data was securely transmitted across the system and stored safely in databases. However, the multi-modal nature of the system introduced additional challenges in managing privacy and user consent. Since multiple forms of data were being collected and processed, users needed to explicitly consent to each individual modality. This raised issues about how to ensure user understanding and consent for each type of data collected. Balancing strong security with respect to user privacy proved to be an ongoing challenge during system development.

Environmental Conditions and System Limitations

Finally, environmental conditions and system limitations presented significant obstacles. In real-world environments, individuals are often walking in less-than-ideal conditions, which introduces challenges such as lighting variations, occlusions, and background noise [16]. These environmental factors can affect the model's ability to accurately recognize gait patterns. For instance, occlusions (where other people or objects block the view of the person's gait) or poor lighting conditions can distort the gait data, reducing the model's accuracy. These issues are particularly prevalent in high-traffic areas or high-security environments, where lighting and camera angles are often suboptimal [16].

In addition to environmental issues, gait variability caused by external factors such as footwear or health conditions further complicated the system's ability to consistently identify individuals. For example, individuals walking in heavy boots or with a limp may

exhibit a gait pattern that significantly differs from their usual walking style. This type of variability posed a challenge because it could lead to misidentifications or failures in authentication, especially when walking conditions changed unexpectedly.

To address these environmental challenges, data augmentation and sensor integration strategies were explored. By integrating additional data sources such as depth sensors, accelerometers, or motion sensors, the system could capture more comprehensive data, making it more robust to environmental factors like poor lighting or occlusions [10]. These sensors could provide valuable insights into the subject's movement, which would improve the accuracy of gait recognition even in challenging real-world environments.

Expanding the training dataset to include more diverse walking conditions, such as different types of footwear, ages, and health conditions, would further help improve the system's ability to generalize. This expansion would ensure that the model performs reliably across a broader range of real-world scenarios, thus improving the system's overall accuracy and reliability.

Future Implementations

As with any cutting-edge technology, the development of the multi-modal biometric authentication system combining gait recognition, mouse dynamics, keystroke dynamics, and voice recognition has opened up numerous exciting avenues for future enhancements and innovations. This section discusses potential future directions for improving the system, including real-time processing, expanding biometric modalities, enhancing model accuracy, and addressing ethical concerns related to privacy and user consent. These improvements will not only ensure that the system can operate effectively in real-world environments but also allow it to scale for broader applications, especially in mission-critical security systems.

Enhancing Real-time Processing and Computational Efficiency

One of the key areas that require significant improvement is real-time processing and computational efficiency. While the current system performs admirably during batch

processing, real-time authentication is essential, particularly in high-security environments such as data centers, government facilities, and corporate enterprises. In these settings, the model's ability to authenticate users continuously as they interact with the system is crucial for maintaining security in dynamic environments where users are always on the move.

At present, the system requires substantial computational resources to process data from multiple biometric modalities (e.g., gait, mouse dynamics, keystroke dynamics, and voice recognition). As the system is intended to operate in mission-critical environments, it is vital to minimize latency and maximize throughput to make the system suitable for practical deployment. To achieve this goal, edge computing should be considered. By processing data locally on edge devices (such as cameras, sensors, and microphones) rather than relying on centralized servers, it would be possible to reduce latency and improve the speed of the authentication process [13]. This would make the system more responsive and capable of making quick authentication decisions in real-time.

Beyond edge computing, optimizing the model architecture itself is critical. Techniques such as model pruning or quantization could be explored to reduce the model's size and make it more computationally efficient without compromising its performance. These strategies could enable the model to process data faster and allow it to scale effectively, making it viable for environments where immediate authentication is required. Improving the real-time processing capability of the system would allow it to seamlessly integrate into high-security environments without introducing delays or creating performance bottlenecks.

Integrating Other Biometric Modalities

While the integration of gait recognition, mouse dynamics, keystroke dynamics, and voice recognition has already proven highly effective in improving authentication accuracy and security, there is substantial potential for further enhancement by incorporating additional biometric modalities [11]. Adding additional forms of identification, such as facial recognition, iris scanning, and fingerprint scanning, could

significantly increase the layers of security offered by the system.

Facial recognition, for example, could be integrated alongside gait recognition to create a multi-layered security system. While gait recognition provides continuous and passive authentication, facial recognition can offer an additional initial check when a user first approaches the system. This dual approach would be particularly valuable in secure entry points, such as access-controlled doors or restricted areas, where a quick facial scan could be performed alongside the gait-based authentication [11]. This combination of authentication techniques would offer enhanced security measure by ensuring both physical presence and behavioral consistency.

In addition to facial recognition, other well-established biometrics like iris scanning and fingerprint recognition could be integrated to further bolster the system's security. Iris scanning, known for its high accuracy and resistance to spoofing, could serve as an additional verification step in environments requiring high-level security [5]. Similarly, fingerprint recognition is a widely adopted and well-trusted modality for identity verification, and its inclusion would offer an additional layer of multi-factor authentication.

By incorporating these additional biometric modalities, the system would be made more resilient to attack vectors, significantly increasing the overall security. This multi-modal approach would be especially vital in environments where unauthorized access could have catastrophic consequences, such as military bases, financial institutions, and government buildings, where multiple forms of authentication would drastically enhance security.

Improving Model Accuracy with Larger Datasets and New Architectures

While the current model performs well with the existing dataset, improving model accuracy and generalization remains a key area of future development. One of the most effective ways to improve system performance is by training the model on larger and more diverse datasets. Currently, the model has been trained primarily using the Shuai

Zheng Gait Dataset, which provides a comprehensive collection of gait patterns from 124 subjects. However, to further enhance the model's ability to recognize a broader range of gait patterns, it is essential to expand the dataset to include more subjects and more varied walking conditions.

Training the system on a more diverse dataset, one that includes individuals of varying ages, ethnicities, body types, and gait styles, would significantly improve its ability to generalize to real-world applications. By exposing the model to a wider variety of walking patterns, the system would be able to better perform across different demographic groups and physical conditions. Additionally, the expanded dataset should include gait data captured under different environmental conditions, such as varying lighting, weather conditions, and occlusions. This would make the model more robust to the variability encountered in real-world environments, ensuring consistent authentication performance.

Beyond expanding the dataset, it would be valuable to explore new deep learning architectures that could further improve the model's ability to recognize gait patterns and integrate multiple biometric modalities. For instance, the Transformer architecture, which has shown remarkable success in tasks related to natural language processing, could be adapted for gait recognition and multi-modal fusion [16]. Capsule Networks, a relatively recent innovation in deep learning, are another promising architecture, especially since they can capture spatial relationships between features more effectively [14]. Experimenting with newer architectures while simultaneously training on more diverse datasets will significantly improve the model's accuracy, efficiency, and generalization, making it even more suitable for mission-critical applications.

Addressing Ethical Concerns and Ensuring Privacy

As biometric systems increasingly process sensitive personal data, including gait patterns, voice recordings, and mouse dynamics, privacy remains a critical concern. The development of any biometric authentication system must consider ethical issues and ensure that user privacy is respected at all stages of the system's operation. User consent

is paramount in ensuring that individuals are fully informed about the collection, storage, and use of their biometric data.

To address privacy concerns, it is essential to implement robust consent protocols that ensure users are aware of how their data is being used and that they can easily opt-out of data collection if they choose to do so. In addition, privacy-preserving machine learning techniques, such as federated learning, could be explored as a means of improving data privacy. In federated learning, data remains on the user's device, and only model updates are shared with a central server, preventing the central server from ever accessing the raw biometric data. This approach can ensure greater privacy for users, as the system will never have access to their actual biometric data, significantly reducing the risk of privacy breaches.

Encryption of data both during storage and transmission is another critical measure to protect sensitive information. By implementing end-to-end encryption, user data will remain secure, preventing unauthorized access or data breaches. As biometric systems are deployed in more real-world settings, ensuring that ethical considerations are addressed throughout the development and deployment stages becomes increasingly important. This includes making sure that informed consent is obtained, that data is stored and processed securely, and that users' privacy rights are always respected. Additionally, the system must comply with data protection regulations such as the GDPR and HIPAA, ensuring that users' personal information is protected and handled appropriately under legal standards [8].

Improving User Experience

The user experience (UX) remains a crucial factor for the system's success. While one of the main benefits of gait-based authentication is its non-intrusive and seamless nature, it is important to ensure that the system remains user-friendly and accurate across a wide range of user behaviors. The system must be able to reliably authenticate users even when they are distracted, moving quickly, or carrying objects. This flexibility is necessary to ensure that the authentication process does not become a hindrance to users

in real-world environments.

To improve user interaction, the system could include real-time feedback. For example, users could receive immediate notifications if the authentication process was successful or if the system failed to authenticate due to changes in gait. This would help to build trust in the system and ensure users understand their authentication status. Further, incorporating intuitive user interfaces (UI) into the system could significantly improve user experience. By designing user-friendly interfaces, the system can reduce friction and improve user satisfaction while ensuring that security is not compromised.

Additionally, the personalization of the system could be explored. For example, users could have the ability to adjust settings or provide feedback on how the authentication process is working. Personalization ensures that the system adapts to different users' needs and environments, thus offering both security and ease of use.

Conclusion

The research conducted in this study demonstrates the potential of a multi-modal biometric authentication system that integrates gait recognition, mouse dynamics, keystroke dynamics, and voice recognition to provide enhanced security for critical systems. The system offers a seamless, continuous, and non-intrusive method of authentication, addressing the limitations of traditional authentication methods like passwords, PIN codes, and even fingerprint scanning. By leveraging gait analysis alongside behavioral biometrics such as mouse movements and keystroke patterns, this system introduces a new paradigm in authentication, where users are continuously verified without needing to actively engage with the system. This research highlights the importance of gait recognition as a powerful modality within this multi-modal framework and underscores its potential to enhance security in high-stakes environments.

Key Findings

One of the key findings from this research is that gait recognition alone, as a biometric

modality, offers significant potential for continuous authentication. The system was trained using the Shuai Zheng Gait Dataset, which enabled it to learn robust representations of gait patterns across 124 subjects. The system achieved a high level of accuracy, with a 90% success rate on the test set, demonstrating its ability to distinguish between different gait patterns even under challenging conditions. This result confirms that gait recognition can serve as a reliable, non-intrusive biometric modality for authentication, especially in critical systems where seamless security is paramount.

The integration of mouse dynamics, keystroke dynamics, and voice recognition further enhanced the authentication accuracy and robustness of the system. While gait recognition alone showed promising results, the multi-modal approach proved to be significantly more effective in reducing false positives and false negatives, common issues in biometric authentication systems. By combining different forms of biometric data, the system was able to account for the variability of each modality and provide redundant layers of verification. This multi-modal fusion makes the system more resilient in real-world applications, where environmental factors, changes in user behavior, and inconsistent biometric patterns can cause issues for single-modality systems.

Furthermore, the multi-modal system demonstrated the ability to authenticate users even when one biometric modality (such as gait) was affected by external factors like lighting conditions or occlusions. For instance, if gait recognition was compromised due to walking conditions or posture variations, the system could fall back on voice recognition or keystroke dynamics, ensuring that the user's identity was still accurately verified. This redundancy in authentication layers highlights the increased security and reliability of the multi-modal approach, making it suitable for high-security environments where user identity must be verified continuously and seamlessly.

Importance of Integrating Gait Analysis for Enhanced Authentication

The integration of gait analysis into the multi-modal biometric authentication system represents a significant step forward in enhancing security. Unlike traditional static biometrics like fingerprints or facial recognition, which can be compromised through

various means (e.g., using fingerprint molds or 3D facial models), gait is inherently dynamic and difficult to replicate [1]. Gait recognition offers the unique advantage of continuously monitoring an individual's walking pattern, providing an ongoing form of authentication. This passive authentication means that users are constantly verified without having to actively engage with the system, making it ideal for high-security environments where unauthorized access must be prevented without interrupting the user's experience [8].

Moreover, gait is a behavioral biometric, meaning it is not influenced by external factors such as age, gender, or ethnicity [15]. This makes gait recognition more inclusive than other forms of biometric authentication, such as facial recognition, which may face challenges due to variations in lighting, aging, or changes in facial appearance. Gait, on the other hand, remains relatively stable across different lighting conditions and environments, and it is unique to each individual. As a result, gait recognition provides an effective way to verify identity without the need for specialized sensors or intrusive interactions.

By integrating gait recognition with other behavioral biometrics, the system improves its accuracy and reliability. Voice recognition, for instance, helps to account for changes in gait due to external factors like walking speed or carrying a heavy load, while mouse dynamics and keystroke dynamics provide complementary data that reinforces the authentication process. This combination of multiple layers of verification ensures that the system remains accurate and secure even in the face of biometric variations, which is a common challenge in biometric-based security systems.

Contributions to the Field

This research makes several significant contributions to the field of behavioral biometrics and security. First and foremost, it validates gait recognition as an effective biometric modality for continuous authentication in high-security systems. While gait recognition has been explored in academic literature, this study provides concrete evidence that it can be used in real-world applications for security. The study demonstrates that gait can be

extracted and utilized as a reliable feature for authentication purposes when combined with other biometric data. This opens up a new avenue for enhancing security protocols, especially for environments that demand constant, seamless authentication without human intervention [15].

Additionally, this research demonstrates the power of multi-modal authentication. While much of the research in biometric authentication has focused on single-modality systems, this study highlights the advantages of combining multiple biometric sources to achieve better accuracy and robustness. The integration of gait, mouse dynamics, keystroke dynamics, and voice recognition represents a novel approach to biometric security, one that addresses the weaknesses of individual modalities and provides a more secure, reliable, and resilient system. This contribution to the field is particularly significant in contexts like data protection, where traditional security systems often fall short in defending against sophisticated attacks.

Moreover, the study offers a framework for real-world deployment, showing how multi-modal biometric systems can be effectively implemented in critical systems that require high levels of security. The results suggest that multi-modal systems are not only effective at enhancing authentication accuracy but also at improving overall system reliability by reducing the risk of false positives and false negatives. By deploying multi-modal systems in real-world scenarios, organizations can ensure that only authorized users gain access to restricted areas and critical resources, making this research highly relevant to industries like cybersecurity, healthcare, government, and finance.

Potential Real-world Applications and Impact on Cybersecurity and Privacy

The potential real-world applications of this multi-modal biometric authentication system are vast and far-reaching. As mentioned earlier, the system is particularly well-suited for high-security environments such as data centers, government buildings, and military installations, where unauthorized access could lead to catastrophic consequences.

Traditional security measures, such as passwords, PIN codes, and access cards, are easily compromised through phishing, social engineering, or theft, whereas gait recognition

offers a more secure, continuous form of authentication. By combining gait recognition with other modalities like voice recognition and keystroke dynamics, organizations can ensure that their systems are protected against unauthorized access and that critical resources remain secure.

The integration of multi-modal biometric systems also has the potential to revolutionize cybersecurity by addressing some of the long-standing vulnerabilities in existing security protocols. In particular, gait-based authentication can help mitigate the risks associated with password-based systems, which are vulnerable to hacking, phishing, and social engineering. By leveraging continuous authentication, organizations can prevent unauthorized access without the need for active user engagement. The system can also help mitigate the risk of insider threats, as it continuously verifies the identity of users even after they have been authenticated.

In terms of privacy, the system was designed to ensure that biometric data is securely stored and that user consent is obtained for data collection and processing. By only storing feature embeddings - compressed representations of biometric data—rather than raw biometric data itself, the system ensures that personal information is protected. This approach aligns with data protection regulations such as GDPR and ensures that users' privacy rights are upheld while maintaining high levels of security [8].

Moreover, voice recognition and gait recognition are non-intrusive and cannot be easily spoofed or replicated, providing stronger security while still respecting user privacy. The combination of these biometric traits offers a secure and privacy-conscious alternative to traditional authentication methods. This approach also helps ensure that personal data is never compromised, providing users with peace of mind and protecting organizations from potential security breaches.

References

- [1] A. Amigud, J. Arnedo-Moreno, T. Daradoumis and A.-E. Guerrero-Roldan, "A Behavioral Biometrics Based and Machine Learning Aided Framework for Academic Integrity in E-Assessment," in *2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS)*, Ostrava, Czech Republic, 2016.
- [2] N. A. Lal, S. Prasad and M. Farik, "A Review Of Authentication Methods," *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, vol. 5, no. 11, 2016.
- [3] Á. M. G.-H. M. Á. G.-S. Claudia Álvarez-Aparicio, A. Campazas-Vega, V. Matellán and C. Fernández-Llamas, "Biometric recognition through gait analysis," 25 08 2022.
- [4] D. Teran, K. Thurnhofer-Hemsi and E. Domínguez, "Human Gait Activity Recognition Using Multimodal Sensors," *International Journal of Neural Systems*, vol. 0, no. 0, 2023.
- [5] K. O. Bailey, J. S. Okolica and G. L. Peterson, "User Identification and Authentication using Multi-Modal Behavioral Biometrics," p. 13, 2014.
- [6] M. Farik and K. Kumar, "A Review Of Multimodal Biometric Authentication Systems," *International Journal of Scientific & Technology Research*, vol. 5, no. 12, 2016.
- [7] Y. B. W. Piugie, "Performance and security evaluation of behavioral biometric systems," 14 03 2024. [Online]. Available: https://theses.hal.science/tel-04504693v1/file/sygal_fusion_48853-wandji_piugie-yris_brice_659fb3979f939.pdf. [Accessed 10 04 2025].
- [8] S. B. Mandlik, R. Labade, S. V. Chaudhari and B. S. Agarkar, "Review of gait recognition systems: approaches and challenges," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 15, no. 1, 2025.
- [9] S. Zheng, J. Zhang, K. Huang and R. He, "Robust view transformation model for gait recognition," in *18th IEEE International Conference on Image Processing, ICIP 2011*, Brussels, Belgium, 2011.
- [10] C. Zhang, W. Liu, H. Ma and H. Fu, "Siamese neural network based gait recognition for human identification," in *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Shanghai, China, 2016.
- [11] S. M. ALGHAMDI, S. K. JARRAYA and F. KATEB, "Enhancing Security in Multimodal Biometric Fusion: Analyzing Adversarial Attacks," p. 13, 25 07 2024.
- [12] G. Pradel, T. Li, D. Pradon and N. Roche, "An Embedded Gait Analysis System for CNS Injury Patients," 09 2019. [Online]. Available:

- https://www.researchgate.net/publication/336154728_An_Embedded_Gait_Analysis_System_for_CNS_Injury_Patients. [Accessed 10 04 2025].
- [13 A. A. Sheth, M. Sharath, A. S. C. Reddy and S. Manjunath, "Gait Recognition Using Convolutional Neural Network," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 19, no. 01, 2023.
- [14 M. Gupta, "Biometric Authentication using Gait Recognition," *Universal Research Reports*, vol. 10, no. 04, 2023.
- [15 L. Ruiz-Ruiz, F. Seco, A. R. Jiménez-Ruiz, E. Aleto, A. Jiménez-Martín and J. J. García-Domínguez, "A Comparative Study of Gait Analysis Technologies," in *2023 13th International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, Nuremberg, Germany, 2023.
- [16 N. P and M. F. Ukrit, "The Systematic Review On Gait Analysis: Trends And Developments," *European Journal of Molecular & Clinical Medicine*, vol. 07, no. 06, 2020.
- [17 D. Maiti and M. Basak, "Multimodal biometric integration: Trends and insights from the past quinquennial," *World Journal of Advanced Research and Reviews*, p. 15, 2024.
- [18 Plurilock, "Behavioral Biometrics," [Online]. Available: <https://plurilock.com/what-is-behavioral-biometrics/>.
- [19 R. Yampolskiy and V. Govindaraju, "Behavioural biometrics: A survey and classification," 01 2008. [Online]. Available: https://www.researchgate.net/publication/247836093_Behavioural_biometrics_A_survey_and_classification.
- [20 V. Munusamy and S. Senthilkumar, "Emerging trends in gait recognition based on deep learning: a survey," 07 2024. [Online]. Available: <https://pmc.ncbi.nlm.nih.gov/articles/PMC11323174/>. [Accessed 05 04 2025].
- [21 W. Fonseca, "Understanding Neural Networks: A Comprehensive Guide," 07 01 2023. [Online]. Available: <https://www.linkedin.com/pulse/understanding-neural-networks-comprehensive-guide-fonseca-/>. [Accessed 01 03 2024].

Sri Lanka Institute of Information Technology.docx

ORIGINALITY REPORT

9%	4%	6%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Mehdi Ghayoumi. "Generative Adversarial Networks in Practice", CRC Press, 2023 Publication	1%
2	Submitted to Sri Lanka Institute of Information Technology Student Paper	1%
3	Shashi Kant Dargar, Shilpi Birla, Abha Dargar, Avtar Singh, D. Ganeshaperumal. "Sustainable Materials and Technologies in VLSI and Information Processing - Proceedings of the 1st International Conference on Sustainable Materials and Technologies in VLSI and Information Processing (SMTVIP, 2024), December 13-14, 2024, Virudhunagar, India", CRC Press, 2025 Publication	1%
4	fastercapital.com Internet Source	<1%
5	Submitted to Liverpool John Moores University Student Paper	<1%
6	de Castro Ferreira, João Pedro. "A Federated Learning Platform for High Speed Distributed Data Streams", Universidade do Porto (Portugal), 2024 Publication	<1%
7	Amol Dattatray Dhaygude, Suman Kumar Swarnkar, Priya Chugh, Yogesh Kumar	<1%

