An AI-Based Gait Authentication Framework Leveraging Swing Phase Dynamics

FRANK (SICONG) CHEN*, Syracuse University, USA
AMITH KAMATH BELMAN, San Jose State University, USA
VIR V. PHOHA, Syracuse University, USA
PRONAB MOHANTY, Inspector General of Police, Government of India, India

Gait signals captured by accelerometers embedded in mobile and wearable devices provide an effective and unobtrusive mechanism for user authentication. While deep neural networks have demonstrated strong performance in gait recognition, manually engineered features offer greater interpretability and deeper insight into the structural dynamics of human walking patterns. In this paper, to the best of our knowledge, we are the first to formally establish a direct relationship between accelerometer signals and specific foot movements. Our analysis reveals a distinctive pattern within the swing phase of the gait cycle that carries significantly greater discriminative power than the stance phase. Motivated by this observation, we propose nine novel features extracted exclusively from the swing phase and systematically evaluate their effectiveness for authentication. An authentication system built on these features achieves a 95.51% correct classification rate and a 4.56% equal error rate, outperforming baseline models that rely on full gait-cycle features. Extensive experimental evaluation and detailed computational algorithms further demonstrate the robustness and reliability of the proposed authentication framework.

CCS Concepts: • **Security and privacy → Biometrics**; • **Human-centered computing → Mobile computing**; **Smartphones**; **Mobile devices**.

Additional Key Words and Phrases: Gait signals and recognition, authentication, AI

ACM Reference Format:
Frank (Sicong) Chen, Amith Kamath Belman, Vir V. Phoha, and Pronab Mohanty. 0. An AI-Based Gait Authentication Framework Leveraging Swing Phase Dynamics. *Digit. Threat. Res. Pract.* 1, 1, Article 111 (0), 16 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

Gait-based user authentication, which leverages gait analysis to capture and analyze unique body movement patterns during walking or running, has gained increasing attention in recent years [33]. Two primary approaches are commonly used: video-based and sensor-based methods. Video-based gait analysis relies on external cameras to capture body movements [22] and utilities computer vision approaches to analyze videos and images to identify walking patterns from silhouette, while sensor-based methods analyze signals collected from wearables or Inertial Measurement Unit (IMU) sensors attached to the body and leverages sensory techniques to analyze patterns

---

[*] This is the corresponding author

Authors' addresses: Frank (Sicong) Chen, frank.chen@dartmouth.edu, Syracuse University, Syracuse, New York, USA; Amith Kamath Belman, amith.kamathbelman@sjsu.edu, San Jose State University, San Jose, California, USA; Vir V. Phoha, vvphoha@syr.edu, Syracuse University, Syracuse, New York, USA; Pronab Mohanty, pronabmohanty@gmail.com, Inspector General of Police, Government of India, New Delhi, Delhi, India.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 0 Copyright held by the owner/author(s). Publication rights licensed to ACM.

2576-5337/0/0-ART111 $15.00
https://doi.org/XXXXXXX.XXXXXXX

from sensor readings. Among sensor-based methods, accelerometers, widely integrated into mobile and wearable devices, have become one of the most popular tools for gait analysis.

Prior research [8, 12, 23] has shown that accelerometer signals exhibit repetitive patterns corresponding to gait cycles, typically defined as two consecutive footsteps. Many studies [3, 28] have leveraged these cycles by detecting their boundaries to create templates or extract features vectors for user authentication. However, template-based approaches rely heavily on the accurate detection of complete gait cycles, making them susceptible to performance degradation under imprecise segmentation, inter-cycle variability, and vulnerable to imitation attacks. [36]. On the other hand, gait authentication methods that rely on statistical features extracted from entire gait cycles, such as cycle length, velocity, and signal extrema (e.g., minimum and maximum values) [3], often overlook critical structural information. Such methods fail to capture the precise locations of peaks and valleys, making them insensitive to the signal's structural fluctuations at key gait events. Consequently, two gait cycles with different shapes may yield similar statistical features, leading to inadequate representation of individual gait patterns and increased vulnerability to imitation attacks.

Gait cycles can be segmented into stance phase and swing phase, or other segments marked by key foot events such as heel contact, heel off, and toe-off [26]. Several studies [4, 24] have attempted to associate heel contact and toe-off events with accelerometer signals to enhance cycle detection and improve feature extraction accuracy. However, these studies have not fully explained (1) why specific foot events correspond to certain points in the accelerometer readings, (2) what foot movements occur within the swing phase, and (3) why accelerometer signals exhibit significant variations during this phase.

Through experimental observations, we identify distinct signal patterns corresponding to key foot movements — foot lift, mid-swing (flight), and foot landing — within the swing phase. Based on these patterns, we propose a structured representation to capture the swing phase and detect these key events from accelerometer signals. We then define nine features associated with these events to represent the structural characteristics of the swing phase and evaluate their discriminative power for user authentication through experiments.

The primary contributions of this work are as follows:

- We identify a distinctive pattern within gait cycles captured by accelerometer signals, specifically highlighting the swing phase as the most informative period for authentication due to its high rate of signal variation compared to the stance phase.
- We propose a set of nine features extracted from the swing phase, which effectively capture key structural variations and discriminative characteristics of gait cycles.
- We evaluate the performance of a gait-based authentication system using these features, achieving an average correct classification rate (CCR) of 95.51% and an equal error rate of 4.56%, surpassing the performance of all gait cycle-based authentication baseline models.

The remainder of this paper is organized as follows: In the *Prior Work* section, we review and compare studies that leverage gait cycles extracted from accelerometer signals for user authentication. Section *Capturing the Swing Phase from Accelerometer Signals* presents our main contribution: the methodology for defining and detecting the swing phase based on accelerometer readings, including how key foot events correspond to key points in the signal. We then describe the extraction and analysis of features from this phase in Section *Extracting and Analyzing Features from the Swing Phase*. The *Experiments* section demonstrates how these features support gait-based user authentication, compares performance with prior work, and evaluates generalizability in the *Discussion* section. Finally, the *Conclusion* summarizes the work and outlines potential extensions of swing phase analysis to other domains.

2 PRIOR WORK

Accelerometer signals have been extensively utilized for gait-based user authentication, with the gait cycle serving as a fundamental analytical unit. Many studies begin by segmenting gait signals into cycles and then perform authentication based on this structure. Existing approaches can be broadly classified into three categories: template-based methods, feature-based methods, and neural network-based methods.

Table 1. Comparison of prior studies on gait authentication and gait cycle analysis.(CRM: Cyclic rotation metric, DTW: Dynamic Time Warping, CNN: Convolutional neural network, LSTM: Long short-term Memory, SVM: Support vector machine)

Study	Type of Method	Analysis on Gait Cycle		Methods Used for Authentication
		Key Foot Events	Structural Info	
Mantyjarvi *et al.* [23]	Template-based	×	×	Correlation, frequency analysis
Rong *et al.* [28]	Template-based	×	×	DTW
Nickel *et al.* [27]	Template-based	×	×	Cycle-based feature vectors
Derawi *et al.* [10]	Template-based	×	×	Cycle detection + CRM
Anwary *et al.* [2, 3]	Template-based	✓	✓	Event-based gait segmentation
Alobaidi *et al.* [1]	Feature-based	×	×	Time and frequency domain features
Anwary *et al.* [2]	Feature-based	✓	Partially	CNN classification
Thang *et al.* [32]	Feature-based	×	×	DTW, FFT + SVM
Derawi [9]	Feature-based	×	×	Machine learning on feature vectors
Bejarano *et al.* [4]	Feature-based	✓	×	Step event-based segmentation
Maqbool *et al.* [24]	Feature-based	✓	×	Event-based gait segmentation
Mufandaidza *et al.* [25]	Neural network-based	×	×	DTW + Neural Network
Gadaleta *et al.* [11]	Neural network-based	×	×	Cycle detection + CNN + SVM
Zhang *et al.* [35]	Neural network-based	×	×	LSTM-based classification
Chen *et al.* [7]	Neural network-based	×	×	Siamese network
Our work	Template+Feature	✓	✓	Machine learning models

2.1 Template-based authentication methods

Template-based authentication methods rely on detecting gait cycles and using them to create templates for recognition. Mantyjarvi *et al.* [23] identified unique patterns in acceleration signals using correlation, frequency-domain analysis, and statistical data distribution. By constructing templates based on these patterns, they achieved an Equal Error Rate (EER) of 7%. Gafurov *et al.* [12] proposed a cycle detection method that assumes local minima in accelerometer signals correspond to the start and end of each gait cycle, with each cycle consisting of two steps. Their method, which used feature vectors derived from six consecutive cycles, achieved an 86.3% recognition rate. Nickel *et al.* [27] refined this approach by integrating an estimated cycle length (typically 800 ms – 1400 ms) and a neighbor search technique to detect cycle boundaries more accurately. They also introduced the Cyclic Rotation Metric (CRM), a similarity measure for authentication, achieving an EER of 5.7%. Rong *et al.* [28] developed a partitioning method and gait recognition algorithm using Dynamic Time Warping (DTW). They identified zero-crossing points following local minima to segment gait cycles and applied a time-warping network to generate gait feature codes for recognition, achieving an EER of 6.7%.

While these methods have demonstrated strong authentication performance, their effectiveness is highly dependent on the accuracy of gait cycle detection. Consequently, greater emphasis is placed on detecting cycle boundaries rather than analyzing the structural characteristics of the gait cycle, which are arguably more critical for user authentication. Furthermore, since gait cycles may be captured at varying sampling rates across devices, the same gait movement can be represented with different temporal resolutions, complicating direct template comparisons. Additionally, higher sampling rates result in more data points per cycle, increasing the computational cost of distance-based matching. These factors make template-based approaches less suitable for real-time authentication on resource-constrained mobile and wearable devices.

2.2 Feature-based authentication methods

To address the limitations of template-based methods, some studies have proposed feature-based approaches that extract key attributes from gait cycles. Alobaidi *et al.* [1] extracted over 300 time- and frequency-domain features, such as mean, standard deviation, and median, to classify activities, reporting an EER of 11.38% for normal walking activity. Anwary *et al.* [2] extracted 12 features from detected gait cycles, including the maximum and minimum accelerometer readings, total time, total velocity, and stride length. They trained a convolutional neural network (CNN) using the extracted feature vectors to classify individuals into young and old groups.

Other researchers have attempted to integrate template-based and feature-based approaches to improve authentication performance. Thang *et al.* [32] proposed two approaches: one using time-domain features with DTW, achieving 79.1% accuracy, and another leveraging Fast Fourier Transform (FFT) and Support Vector Machines (SVM), achieving a Correct Classification Rate (CCR) of 92.7%. Derawi [9] introduced a smartphone-based gait authentication method that combined raw cycle data with features extracted from fixed-length segments. Using machine learning models, their system achieved an EER between 6% and 7%.

While extracting statistical features from signals is a common approach for capturing key information, it often fails to preserve the structural characteristics of the signal, such as the location of peaks and valleys, overall shape, and temporal variations. In biometrics, particularly gait analysis, these unique features are crucial for distinguishing between individuals and should be effectively captured and utilized to enhance recognition accuracy.

2.3 Deep learning-based authentication methods

In recent years, deep learning-based methods have gained significant traction in accelerometer-based gait authentication. Rather than relying on gait cycles, some researchers have explored allowing deep learning models to automatically learn discriminative patterns from arbitrarily segmented gait sequences. For example, Zhang *et al.* [35] proposed an authentication model based on Long Short-Term Memory (LSTM) networks trained on raw accelerometer data, reporting 97.5% and 100% classification accuracy on two different datasets. Similarly, Chen *et al.* [7] implemented a Siamese network consisting of two identical neural branches to learn representations from 2-second gait segments, achieving a classification accuracy of up to 90.42%.

While these deep learning-based approaches have demonstrated strong authentication performance, they typically operate on fixed-length windows that are not explicitly aligned with biomechanically meaningful segments such as gait cycles or other key foot events during walking. Although layers such as CNNs can implicitly capture structural patterns in gait signals, the lack of explicit alignment may hinder interpretability and make it harder to relate learned representations to specific gait dynamics. Gadaleta *et al.* [11] attempted to address this by detecting gait cycles before applying a CNN model for feature extraction, suggesting that incorporating explicit gait cycle information can help enhance the interpretability of deep learning-based models.

2.4 Enhancing digital security through AI techniques

Artificial intelligence has become a key enabler of modern digital security systems[5, 21, 34]. At the foundational level, Shi *et al.* [29] presented mathematical foundations of machine learning, which underpin the theoretical rigor of modern AI systems used in digital security frameworks. Iyengar *et al.* [19] further provided a comprehensive treatment of AI methodologies applied to cybersecurity and digital forensics, offering both theoretical perspectives and real-world implementations. From an architectural and deployment standpoint, Singaram *et al.* [30] discussed the design, development, and deployment of deep learning networks, offering practical insights into scalable AI architectures applicable to secure digital ecosystems. Soni *et al.* [31] provided a comparative analysis of deep learning models for image super-resolution, highlighting how generative enhancement techniques can introduce new challenges for forensic and security systems.

Temporal modeling plays a central role in AI-driven security, particularly for sequential and behavioral data. Hariprasad *et al.* [18] introduced boundary-based fake face anomaly detection using recurrent neural networks, establishing early AI-driven temporal modeling approaches for detecting synthetic artifacts. Iyengar *et al.* [20] further explored temporal deepfake generation and detection using RNNs, reinforcing the importance of sequence modeling for adversarial content detection. Hariprasad *et al.* [17] developed an AI-based anomaly detection technique focusing on lip-region analysis for deepfake video detection, highlighting fine-grained spatial-temporal feature extraction for improved detection accuracy.

Beyond detection, AI techniques have also been integrated with broader security mechanisms [14, 15]. Hariprasad *et al.* [16] proposed advanced encryption mechanisms for quantum-safe video transmission, addressing secure data transmission alongside intelligent analysis. Gupta *et al.* [13] presented a dual-paradigm AI framework integrating pre- and post-quantum-trained neural networks for robust deepfake detection, demonstrating how AI models can be designed to remain resilient under emerging quantum-era threats. These studies highlighted how AI-driven temporal modeling, robust architecture design, and system-level security considerations contribute to resilient digital security solutions, providing useful context for accelerometer-based gait authentication systems that rely on sequential signal modeling and robustness against adversarial or environmental variations.

2.5 Exploring structural information in gait cycles

Gait cycles can be further segmented into stance and swing phases, with key events such as heel contact (HC) and toe-off (TO) marking their transitions [26]. These events are essential for precise gait cycle segmentation and provide insights into structural information. Bejarano *et al.* [4] and Maqbool *et al.* [24] identified HC and TO events within accelerometer signals to improve gait cycle detection and velocity estimation. However, additional micro-movements—such as foot raising, flight, and lowering—also contribute to signal variations during the swing phase but remain largely unexplored.

A few studies have investigated these finer details within gait cycles. Anwary *et al.* [2, 3] identified eight foot events in accelerometer signals collected from shoe-mounted sensors. They observed that the most significant signal variations occur during the swing phase and leveraged this insight to segment stance and swing phases for step detection. Their findings suggested that swing phase analysis could improve step length and velocity estimation. However, their study focused primarily on terminal stance and TO event detection without fully analyzing how variations in accelerometer signals correspond to specific gait events.

Given that the swing phase exhibits higher signal variability and accounts for only 40% of the gait cycle, it presents an opportunity to discard 60% of less important data (stance phase) to improve authentication efficiency. Thus, in this paper, we present a systematic analysis of accelerometer signals during the swing phase, identifying key sub-phases that correspond to specific foot movements. Unlike prior studies that rely on entire gait cycles to create templates or features, or deep learning-based black-box models, we explicitly define and justify the structural changes in accelerometer signals within the swing phase. By leveraging this information-rich phase, we introduce nine features that effectively capture gait pattern for authentication. Our approach improves recognition efficiency by discarding the stance phase while maintaining high discriminative power, offering a computationally efficient and interpretable alternative to existing gait authentication methods.

3 CAPTURING THE SWING PHASE FROM ACCELEROMETER SIGNALS

To analyze gait dynamics and demonstrate our findings, we selected a representative subject (subject 3) from the SU-AIS BBMAS dataset [6] and visualized the accelerometer signals in Figure 1. The top panel of Figure 1 displays the x-axis accelerometer signal ("Acc_X"), revealing a repetitive pattern characteristic of gait cycles, consistent with prior findings by Mantyjarvi *et al.* [23]. The middle panel provides a zoomed-in view of a single gait cycle, illustrating its structure. As noted by Anwary *et al.* [2], accelerometer signals collected from shoe-mounted sensors exhibit relatively stable values during the stance phase and more pronounced fluctuations during the swing phase. Although the dataset used in this study collects accelerometer signals from mobile phones placed in pant pockets, a similar pattern is observed: the stance phase corresponds to a stable segment, while the swing phase corresponds to a fluctuating segment. This consistency suggests that such patterns are not dependent on sensor placement but rather reflect intrinsic leg movements during walking.

This phenomenon can be explained by examining foot dynamics during gait. As illustrated in the bottom panel of Figure 1, the stance phase involves continuous ground contact, leading to minimal variance in accelerometer signals. In contrast, the swing phase, which is initiated at the toe-off (TO) event, occurs when the foot is airborne, resulting in acceleration in all three axes captured by accelerometer. Variations in foot velocity, flight height, and acceleration during this phase lead to significant fluctuations in the accelerometer readings. These variations are highly individual-specific, making the swing phase a informative segment for user authentication. This observation motivates our investigation into whether accurate gait authentication can be achieved using only the swing phase data, as it encapsulates the most distinctive motion patterns within a gait cycle.

3.1 Identifying the swing phase through key foot events in accelerometer signals

To capture the swing phase from accelerometer signals, we define five key points based on local extrema that correspond to biomechanically meaningful foot events, as shown in Figure 1. The swing phase begins at the initial local minimum, TO (Toe-Off), where the foot is about to lift off the ground and starts accelerating forward and upward, resulting in an increase in the accelerometer readings. This is followed by a local maximum, $P1$, representing peak upward acceleration. As the foot reaches its maximum height at mid-swing (MS), the signal descends to a local minimum, reflecting deceleration in the upward trajectory.

After the MS point, the foot accelerates downward, leading to a second peak ($P2$) characterized by another increase in the accelerometer readings. Finally, it decelerates again as it approaches ground contact, ending at the local minimum HC (Heel Contact). This sequence—TO, $P1$, MS, $P2$, and HC—captures a double acceleration–deceleration pattern that aligns with foot dynamics during the swing phase, which remains consistent across subjects and forms the basis for extracting discriminative features for user authentication.

3.2 Structure capturing the swing phase across all axes

While the structured acceleration–deceleration pattern is most prominent along the x-axis (Acc_X), which represents the forward walking direction, it reflects the overall foot dynamics during the swing phase and should therefore also manifest along the other two axes. In the dataset used in this study, accelerometer signals were collected from a mobile phone placed in the pant pocket, where the Acc_X aligns with the forward direction of movement, the y-axis (Acc_Y) aligns along the leg, and the z-axis (Acc_Z) is perpendicular to the body. To investigate whether the swing phase can also be detected in the Acc_Y and Acc_Z signals, we examined their patterns and plot the accelerometer reading from the same subject. As illustrated in Figure 2, a similar structured pattern comprising two peaks and three valleys is also observed in the Acc_Y and Acc_Z readings, corresponding to the swing phase. This suggests that the double acceleration–deceleration dynamics are not limited to forward motion alone, but characterize the broader three-dimensional foot movement during gait.

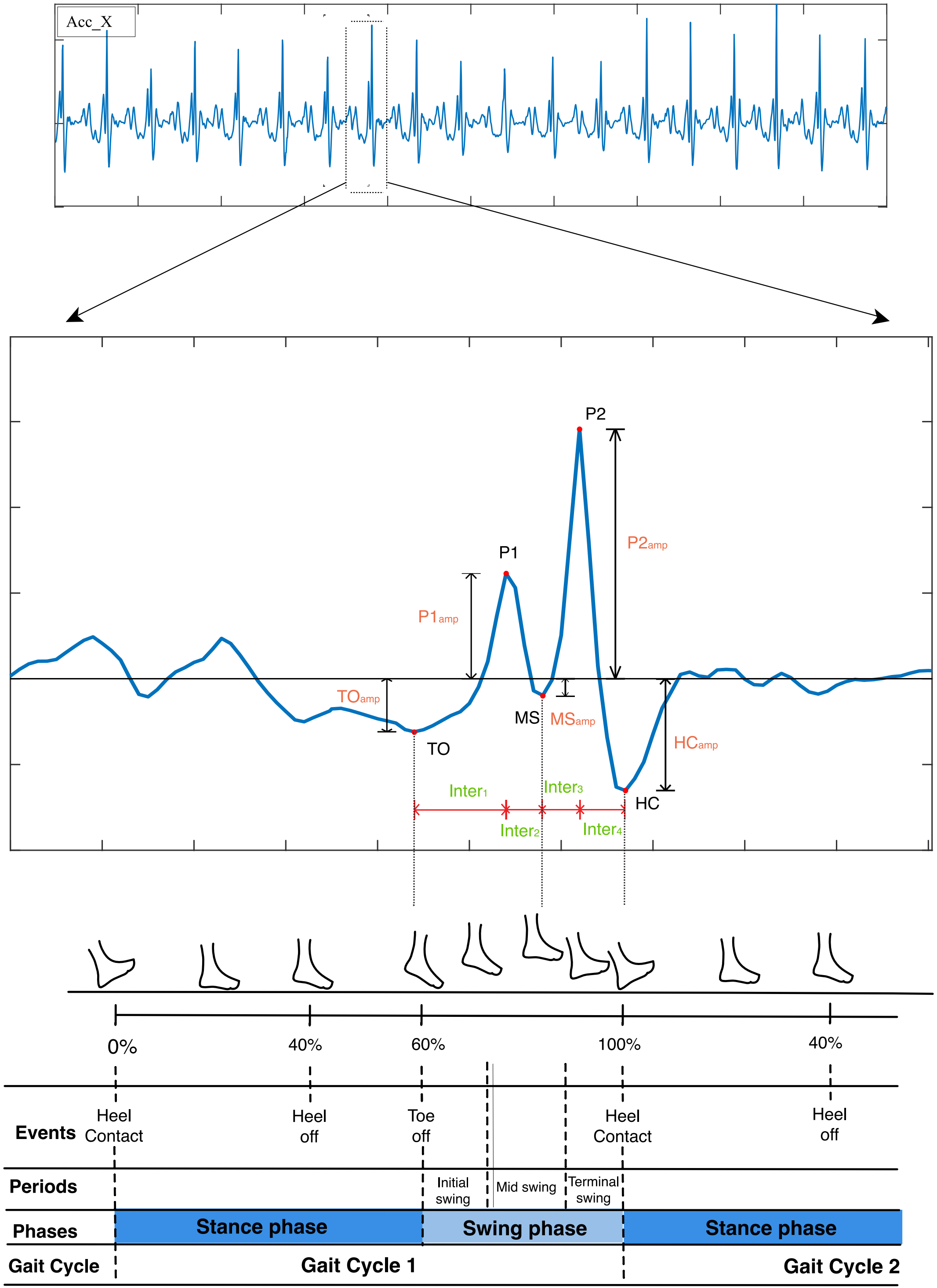
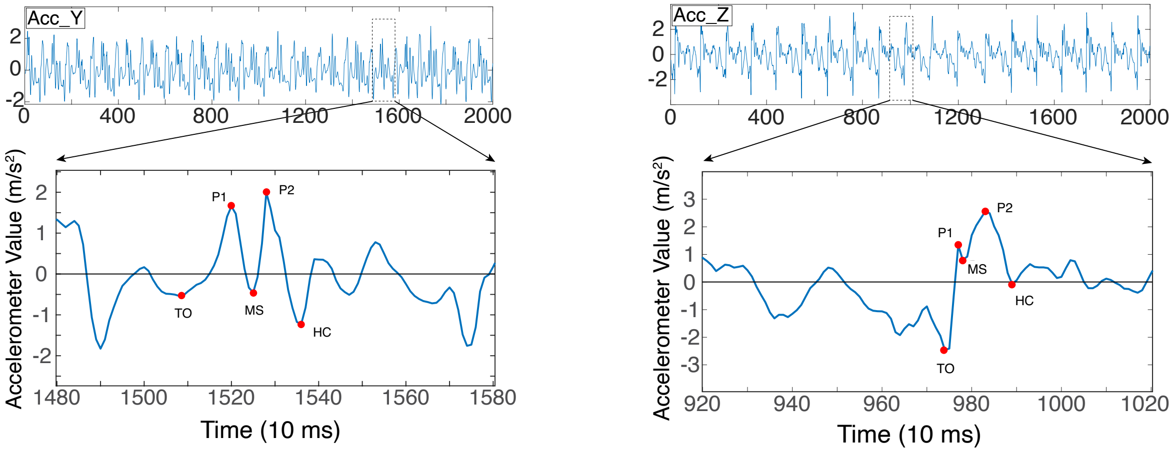


Fig. 1. (Top): Accelerometer signal ("Acc_X") plot from subject 3. (Middle): A zoomed-in view of a single gait cycle from "Acc_X", highlighting the swing phase and key extracted features. (Bottom): Foot events and phases within a gait cycle.



(a) Plot of accelerometer signal ("Acc_Y") from subject 3.

(b) Plot of accelerometer signal ("Acc_Z") from subject 3.

Fig. 2. (Left): Accelerometer signal ("Acc_Y") plot. (Right): Accelerometer signal ("Acc_Z") plot from subject 3. For each figure, the top panel shows the accelerometer signal, while the bottom panel highlights the swing phase structure with annotated key points.

Table 2. Amplitude and temporal features extracted from the swing phase

Amplitude Features (m/s^2)	**Temporal Features**
TO_{amp}: Amplitude of TO	$Inter_1$: Interval between TO and $P1$
$P1_{amp}$: Amplitude of $P1$	$Inter_2$: Interval between $P1$ and MS
MS_{amp}: Amplitude of MS	$Inter_3$: Interval between MS and $P2$
$P2_{amp}$: Amplitude of $P2$	$Inter_4$: Interval between $P2$ and HC
HC_{amp}: Amplitude of HC	

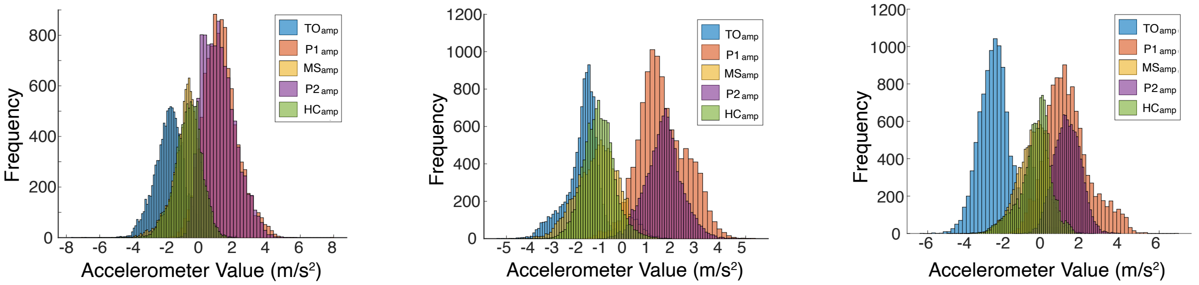
3.3 Detecting the swing phase in accelerometer signals

Given that the swing phase begins at a local minimum and follows a characteristic pattern of alternating valleys and peaks, we employ a three-step procedure to detect it from accelerometer signals.

Step 1: Identifying the start of the swing phase (TO) from Acc_Z (perpendicular to the body). We first locate the TO point by searching for a local minimum within a fixed-length window of 800–1400 ms in the Acc_Z. This window length corresponds to a typical gait cycle duration [10] and ensures that at most one local minimum is captured. In cases where multiple consecutive local minima appear, which might be a result of smoothing techniques, we select the first minimum. It should be noted that although TO appears as a local minimum across all three axes, we found it more reliably detected in the Acc_Z. This may be because the Acc_Z, being perpendicular to the body, reflects horizontal motion and is more influenced by individual body structure (e.g., hip width) rather than in-air foot movements, making the TO event more pronounced.

Step 2: Identifying TO from the other axes. After identifying TO in Acc_Z, we apply a narrower search window (10–15 ms) around the same timestamp in the Acc_X and Acc_Y signals to locate the corresponding TO points. This adjustment accounts for minor misalignment between axes observed in our experiments.

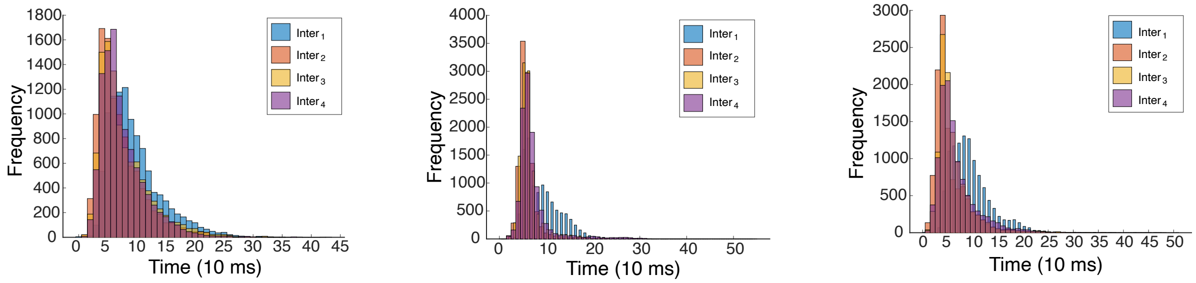
Step 3: Extracting key points within the swing phase. Once TO is determined, we detect subsequent local extrema in each axis to identify $P1$, MS, $P2$, and HC. If multiple consecutive extrema are found, the first occurrence is selected in each case. This sequence of points captures the structured dynamics of the swing phase across all axes.



(a) Amplitude features on Acc_X.

(b) Amplitude features on Acc_Y.

(c) Amplitude features on Acc_Z.



(d) Interval features on Acc_X.

(e) Interval features on Acc_Y.

(f) Interval features on Acc_Z.

Fig. 3. Histogram plots for features from the swing phase structure. The upper row represents amplitude features, while the lower row represents interval features. Amplitude features exhibit a wider spread of distributions, whereas interval features have a narrow spread, are right-skewed, and share a large region of overlap.

4 EXTRACTING AND ANALYZING FEATURES FROM THE SWING PHASE

To capture the structural characteristics of the swing phase, we defined nine features based on the key gait events described in the previous section. The double acceleration–deceleration pattern observed during the swing phase reflects individualized foot dynamics that vary across users. By identifying key points within this pattern, we extract both amplitude and temporal features that quantitatively represent this structure, as illustrated in the middle panel of Figure 1 and summarized in Table 2.

The amplitude features represent the maximum and minimum acceleration values at specific gait events, capturing the intensity and variation in foot movement. These values reflect how forcefully or smoothly the foot accelerates or decelerates during each segment of the swing phase. The temporal features, defined as time intervals between successive key points, indicate how long each movement phase lasts. More importantly, they capture the temporal structure of the swing phase, revealing the relative timing and coordination between foot events. These amplitude and temporal features together provide a comprehensive representation of the swing phase's structure, enabling effective and interpretable user authentication.

To determine which features are more discriminative in distinguishing subjects, we analyze them by plotting their histograms in Figure 3. It is evident that for temporal features across all three axes, as shown in Figures 3d, 3e, and 3f, their distributions are highly similar and exhibit substantial overlap. The spread of these distributions is narrow, and there is significant intersection among them. Additionally, the distributions are asymmetric, with a right-skewed tendency. These observations suggest that temporal features may not be highly discriminative for user authentication.

In contrast, amplitude features, as shown in Figures 3a, 3b, and 3c, exhibit distinct distributions. Their centers are clearly separated, and they do not share too many similar values, especially for features along the y-axis. Additionally, the spread of amplitude distributions is broader, with a wider range compared to temporal features. These findings suggest that amplitude features may provide more distinctive information than temporal features, making them more effective for distinguishing different individuals. Furthermore, features along the y-axis exhibit greater variability than those along the other two axes.

To validate this hypothesis, we define three feature sets and evaluate their classification performance in the following section:

- Feature set 1 (only includes five amplitude features): TO_{amp}, $P1_{amp}$, MS_{amp}, $P2_{amp}$, HC_{amp}.
- Feature set 2 (only contains four temporal features): $Inter_1$, $Inter_2$, $Inter_3$, $Inter_4$.
- Feature set 3 (contains all nine features): feature set 1 + feature set 2.

5 EXPERIMENTS

In this section, we develop an accelerometer-based gait user authentication system using the nine features extracted from the swing phase. By evaluating different feature sets, we assess their discriminative power for user authentication and compare the system's performance with other gait authentication models that rely on full gait cycles.

Table 3. Performance comparison between our method and prior studies. (DTW: Dynamic Time Warping, CRM: Cyclic Rotation Metric, HMMs: Hidden Markov Models)

Study	Classification Method	No. of Subjects	No. of Features	Performance
Gafurov *et al.* [12]	Absolute Distance	50	100	86.3% (CCR)
Derawi *et al.* [10]	DTW & CRM	60	100	5.7% (EER)
Rong *et al.* [28]	DTW	35	Not mentioned	6.7% (EER)
Thang *et al.* [32]	DTW	11	40	79.1% (CCR)
Nickel *et al.* [27]	HMMs	48	52	15.46% (EER)
Gadaleta *et al.* [11]	CNN + SVM	79	40	56.53% (CCR) / 36.66% (EER)
Chen *et al.* [7]	Siamese network	79	128	90.42% (CCR) / 10.34% (EER)
Our work	SVM	79	9	95.51% (CCR) / 4.58% (EER)

5.1 Data description and pre-processing

We use the SU-AIS BB-MAS dataset [6] in our experiments, a publicly available dataset from IEEE Dataport. It contains multiple types of biometric data from 117 subjects, including accelerometer and gyroscope signals for gait, keystroke dynamics, and mobile phone swiping patterns. We use only the accelerometer data collected during walking tasks to train and evaluate our authentication system.

This dataset includes five walking tasks, from which we select the following three tasks where subjects walk on flat ground, ensuring more consistent gait cycles:

- Task 1: Subjects walk along a corridor for approximately 20 seconds after leaving the lab.
- Task 3: Subjects walk in a long corridor for about 60 seconds.
- Task 5: Subjects return to the first corridor and walk back to the lab for approximately 20 seconds.

During data collection, a mobile phone was placed in the subject's pants pocket, with its built-in Android linear accelerometer sensor recording acceleration forces (with the gravity component removed by the Android sensor fusion algorithm) along the x, y, and z axes at a sampling frequency of 100 Hz. The collection process is repeated on two separate days, called Session 1 and Session 2, respectively.

For data pre-processing, we first check the data integrity for all subjects and remove those with incomplete data. We then extract only Tasks 1, 3, and 5 from the remaining dataset, discarding subjects with fewer than 400 samples (equivalent to 4 seconds of data). These cases typically contain only two or three gait cycles, which are insufficient for capturing consistent and observable walking patterns. After filtering, 79 subjects remain in the dataset.

We normalize the accelerometer data along each axis using z-score normalization (zero mean and unit variance). To reduce noise, we apply a moving average filter with a sliding window of 4 seconds (400 points). We then extract nine features from each detected swing phase and label the samples: genuine subjects are assigned a label of 0, while impostors are assigned a label of 1. We use data from Session 1 for training, and data from Session 2 for testing.

Table 4. The average CCR and EER (values in parentheses) for each axis and feature set using LDA and SVM. All values are percentages. Feature Set 1 includes all five amplitude features, Feature Set 2 includes all four interval features, and Feature Set 3 includes all nine features.

	Feature Set 1		Feature Set 2		Feature Set 3	
	LDA	SVM	LDA	SVM	LDA	SVM
Acc_X	86.26 (13.72)	86.37 (13.61)	79.97 (20.15)	80.90 (19.25)	88.48 (11.40)	88.12 (11.79)
Acc_Y	92.47 (7.66)	92.70 (7.42)	90.00 (10.11)	90.33 (9.77)	95.12 (4.97)	95.51 (4.58)
Acc_Z	91.74 (8.45)	91.68 (8.45)	85.05 (15.15)	86.41 (13.76)	94.43 (5.65)	94.06 (6.02)

5.2 Selection of baselines

For comparison, we include three representative template-based studies [10, 12, 28] and two representative feature-based gait authentication studies [27, 32] published between 2007 and 2012. These earlier methods are widely cited and provide baseline performance benchmarks for traditional gait cycle-based approaches. Their performance results are taken directly from the original papers, as the implementation details are insufficient for faithful reproduction.

In addition, we selected two deep learning-based baselines to compare our method against state-of-the-art approaches. The first is the method by Gadaleta *et al.* [11], which segments gait cycles from accelerometer signals and applies a CNN-based feature extractor to learn representations from these cycles, followed by an SVM classifier for authentication. This approach integrates gait cycle analysis with deep learning, aiming to preserve interpretability while benefiting from automated feature learning. The second baseline is a more recent model [7], which employs a Siamese neural network trained on fixed-length (2-second) gait segments to learn similarity-based representations. We re-implemented both methods and evaluated them under the same experimental settings as our proposed model to enable a fair and consistent comparison.

5.3 Experiment evaluation and insights

We trained Linear Discriminant Analysis (LDA) and Support Vector Machine (SVM) classifiers separately for each pair of subjects on each feature set. SVM was trained using a linear kernel with a box constraint of 1 and automatic kernel scaling, while LDA was configured with a linear discriminant type and no regularization (gamma = 0). These parameters were not tuned, as the primary goal of this experiment is to validate the effectiveness of the proposed features rather than to optimize classifier performance. The performance of our authentication system is evaluated using Correct Classification Rate (CCR) and Equal Error Rate (EER).

Table 3 presents the performance comparison between our approach and baseline methods. The upper section reports results from earlier studies, representing baseline performance from traditional gait cycle-based approaches. Our method achieves a CCR of 95.51% and an EER of 4.58%, outperforming all listed baselines. Notably, our approach uses significantly fewer features while being evaluated on the largest dataset among these studies, demonstrating both efficiency and generalizability.

The lower section of Table 3 presents the results of Gadaleta *et al.* [11] and Chen *et al.* [7]. Our swing phase-based model outperforms both baselines, with particularly notable improvements over the method proposed by Gadaleta *et al.*. Although this baseline reported strong performance in its original study, its reduced effectiveness in our evaluation may be attributed to differences in data characteristics and dataset size. Specifically, their method relies on high-resolution, interpolated data collected over multiple extended sessions (approximately five minutes each), enabling the extraction of finer-grained gait cycles and providing sufficient input to effectively train the CNN feature extractor.

In contrast, our nine swing phase-based features explicitly capture the most representative and biomechanically meaningful structures within each gait cycle, allowing traditional machine learning models, like LDA and SVM, to distinguish users with higher reliability. By focusing on interpretable foot movement patterns during the swing phase, our approach delivers a compact, discriminative, and robust representation of gait. This leads to better generalizability and efficiency, particularly in settings with limited data.

In addition to comparing with baseline models, we further evaluate authentication performance using different feature sets and classifiers to examine whether the results align with the analysis presented in the previous section. The performance results are summarized in Table 4. From these results, we make the following key observations:

Observation 1: Amplitude features perform better than temporal features. Feature Set 1 outperforms Feature Set 2 in both CCR and EER across all axes. This result confirms our hypothesis in the previous section that amplitude features are more distinctive due to their broader ranges and distributions. This finding suggests that when computational resources are limited, especially on wearable devices, using only five amplitude features can still achieve reliable authentication performance.

Observation 2: "Acc_Y" and "Acc_Z" outperform "Acc_X". Performance on the y-axis and z-axis is consistently better than on the x-axis. When a mobile phone is placed in a pants pocket, the accelerometer's x-axis aligns with the walking direction, the y-axis aligns along the leg, and the z-axis is perpendicular to the body. These results indicate that walking patterns are less pronounced along the forward direction, while variations in foot lift (y-axis) and waist movement (z-axis) provide more distinctive gait characteristics. These discriminative characteristics are fully captured by the swing phase and our proposed features.

Observation 3: LDA and SVM yield similar performance. Our authentication system achieves 95.51% CCR using nine features with an SVM classifier, and 95.12% CCR with an LDA classifier. Similar performance persists across all cases, suggesting that the extracted features contain sufficient discriminative information, enabling conventional classifiers to outperform prior studies based on the complete gait cycles.

In addition to the evaluated performance, our approach is computationally lightweight and well suited for integration into mobile or wearable systems. The swing-phase detection, which primarily relies on peak and valley detection, can be efficiently implemented using modern signal processing libraries with minimal latency, and both classifiers used in this study are computationally inexpensive during inference. Therefore, our method can operate in near real time on resource-constrained devices without significant energy or memory overhead.

6 DISCUSSION

Although the structured representation of the swing phase has demonstrated promising performance for user authentication, our experiments were conducted under controlled conditions, that is, on flat ground and at normal walking speed. To ensure broader applicability, it is important to examine how this approach generalizes to diverse real-world scenarios. In this section, we discuss three key factors that may influence its performance and explore potential strategies to mitigate their impact.

6.1 Sensor placement

While our study focuses on accelerometer data collected from mobile phones placed in pant pockets, similar swing-phase structures have also been observed in prior studies where sensors were mounted on the shoes [2, 3]. This suggests that the structured double acceleration–deceleration pattern during the swing phase can be consistently captured as long as the sensor is located on or near the leg. However, sensor placement can influence the signal characteristics, particularly with respect to the axis used for identifying the toe-off (TO) point. As discussed in subsection *Detecting the Swing Phase in Accelerometer Signals*, the Acc_Z axis, which is perpendicular to the body, offers a clear and distinctive local minimum for detecting the TO event due to its relative insensitivity to foot movement. When the sensor is placed on the shoes, however, this axis may become less reliable due to increased sensitivity to foot dynamics. In such cases, alternative reference axes, such as the forward walking direction (Acc_X), the vertical axis relative to the ground (Acc_Y), or even a combination of all three axes ($\sqrt{x^2 + y^2 + z^2}$) may provide more robust cues for detecting the TO point.

6.2 Walking speed and sampling rate

Walking speed can affect the features extracted to characterize the swing-phase structure. In particular, the temporal features, which are defined as the durations between key gait events, are sensitive to changes in gait tempo. For example, when a user walks at a faster pace, these intervals naturally shorten, which may reduce their discriminative power. This issue is further exacerbated when data are collected at lower sampling rates, as the resulting intervals may become too brief to distinguish reliably. To mitigate this limitation, additional features such as the slope between adjacent key points can be introduced. These slope features represent the rate of change in acceleration and offer a complementary perspective that is more robust to timing compression caused by increased walking speed.

6.3 Other factors and future work

In addition to sensor placement and walking speed, several other real-world factors may influence the captured gait structure and the extracted features. These include variations in walking surfaces (e.g., hard floors, soft carpets, or uneven terrain), walking on stairs or slopes, and changes in the individual's physical or cognitive state, such as fatigue, intoxication, or distraction. While the dataset used in this study did not capture all possible variations, its consistent performance across more than 80 subjects, collected over multiple days, demonstrates robustness and generalizability to inter-subject and temporal variations. Future work will focus on collecting and analyzing data across a broader range of real-world settings to further validate and enhance the generalizability of the proposed method.

6.4 Security and spoofing robustness

From a security perspective, potential spoofing attacks on gait authentication systems often rely on reproducing the entire gait cycle [36] or synthesizing statistical distributions derived from entire gait cycles. In contrast, our method extracts structural features specifically from the swing phase, where signal dynamics exhibit distinctive and user-specific acceleration–deceleration patterns. Because these localized structural variations differ substantially from global statistical distributions, the proposed approach is expected to provide stronger resistance to feature-level spoofing or imitation attacks.

7 CONCLUSION

In this paper, we introduced a novel approach for accelerometer-based gait user authentication by focusing on the swing phase of the gait cycle. Unlike traditional methods that rely on full gait cycles, our work demonstrates that the swing phase contains the most distinctive movement characteristics, making it highly effective for user authentication. We systematically analyzed the structural variations within the swing phase and extracted nine key features, consisting of five amplitude features and four temporal features.

Through extensive experiments, we evaluated the effectiveness of these features and compared our model with existing gait cycle-based user authentication methods. The experimental results show that our approach outperforms prior works while using significantly fewer features. The findings indicate that amplitude features are more discriminative than temporal features, and that variations along the y-axis and z-axis provide more informative cues for user authentication than those along the x-axis. Additionally, the results indicate that even simple classifiers such as LDA and SVM can achieve high classification accuracy with our proposed features, further demonstrating their robustness and effectiveness.

The insights from this paper emphasize that capturing biomechanically meaningful structures in gait dynamics not only enhances interpretability but also yields superior performance compared to approaches that rely on fixed-length data windows, as commonly seen in emerging deep learning-based methods. Our findings demonstrate that the swing phase offers a computationally efficient and interpretable alternative to black-box models. This contributes to the broader field of biometric authentication by presenting a lightweight yet effective solution well-suited for real-world deployment, especially on resource-constrained wearable devices.

Beyond validating the generalizability of the structured swing phase and proposed features in real-world scenarios discussed in the previous section, we also aim to explore their applications beyond user authentication. In particular, we plan to investigate their potential for estimating physiological attributes such as age, height, and body composition. These factors are critical in forensic investigations. As gait is inherently shaped by an individual's biomechanical structure, these features may provide valuable insights for identity verification, profiling, and forensic gait analysis in surveillance settings.

REFERENCES

[1] Hind Alobaidi, Nathan Clarke, Fudong Li, and Abdulrahman Alruban. 2022. Real-world smartphone-based gait recognition. *Computers & Security* 113 (2022), 102557.

[2] Arif Reza Anwary, Damla Arifoglu, Michael Jones, Michael Vassallo, and Hamid Bouchachia. 2021. Insole-based real-time gait analysis: Feature extraction and classification. In *2021 IEEE International Symposium on Inertial Sensors and Systems (INERTIAL)*. IEEE, 1–4.

[3] Arif Reza Anwary, Hongnian Yu, and Michael Vassallo. 2018. An automatic gait feature extraction method for identifying gait asymmetry using wearable sensors. *Sensors* 18, 2 (2018), 676.

[4] Noelia Chia Bejarano, Emilia Ambrosini, Alessandra Pedrocchi, Giancarlo Ferrigno, Marco Monticone, and Simona Ferrante. 2014. A novel adaptive, real-time algorithm to detect gait events from wearable sensors. *IEEE transactions on neural systems and rehabilitation engineering* 23, 3 (2014), 413–422.

[5] Amith K Belman, Tirthankar Paul, Li Wang, SS Iyengar, Paweł Śniatała, Zhanpeng Jin, Vir V Phoha, Seppo Vainio, and Juha Roning. 2020. Authentication by mapping keystrokes to music: The melody of typing. In *2020 International Conference on Artificial Intelligence and Signal Processing (AISP)*. IEEE, 1–6.

[6] Amith K Belman, Li Wang, Sundaraja S Iyengar, Pawel Sniatala, Robert Wright, Robert Dora, Jacob Baldwin, Zhanpeng Jin, and Vir V Phoha. 2019. SU-AIS BB-MAS (Syracuse University and Assured Information Security—Behavioral Biometrics Multi-device and multi-Activity data from Same users) Dataset. *IEEE Dataport* 10 (2019).

[7] Frank Chen, Jingyu Xin, and Vir V Phoha. 2024. Sspra: A robust approach to continuous authentication amidst real-world adversarial challenges. *IEEE Transactions on Biometrics, Behavior, and Identity Science* 6, 2 (2024), 245–260.

[8] Sicong Chen. 2025. *Enhancing Security and Healthcare Through Continuous Monitoring on Wearable Devices.* Ph. D. Dissertation. Syracuse University.

[9] Mohammad Derawi. 2012. Accelerometer-based biometric gait recognition for authentication on smartphones. (2012).

[10] Mohammad O Derawi, Patrick Bours, and Kjetil Holien. 2010. Improved cycle detection for accelerometer based gait authentication. In *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE, 312–317.

[11] Matteo Gadaleta and Michele Rossi. 2018. Idnet: Smartphone-based gait recognition with convolutional neural networks. *Pattern Recognition* 74 (2018), 25–37.

[12] Davrondzhon Gafurov, Einar Snekkenes, and Patrick Bours. 2007. Gait authentication and identification using wearable accelerometer sensor. In *2007 IEEE workshop on automatic identification advanced technologies*. IEEE, 220–225.

[13] S. Gupta, Y. Hariprasad, S. S. Iyengar, S. Gurappa, and P. Mohanty. 2026. Enhancing Digital Security: A Novel Dual-Paradigm Approach for Robust Deepfake Detection Using Pre- and Post-Quantum-Trained Neural Networks. *ACM Digital Threats: Research and Practice* (2026). To appear, January 2026.

[14] S. Gurappa, Y. Hariprasad, S. S. Iyengar, and N. Chaudhary. 2025. Botnet Detection on CTU-13 Using Lightweight Machine Learning Models. In *Proceedings of the Fourth International Conference on Information Security, Privacy and Digital Forensics (ICISPD 2025).* In press.

[15] S. Gurappa, T. Satharasi, Y. Hariprasad, and S. S. Iyengar. 2025. MedSR-Vision: Deep learning framework for multi-domain medical image super-resolution. In *Proceedings of the 12th Annual Conference on Computational Science and Computational Intelligence (CSCI'25).* In press.

[16] Yashas Hariprasad, SS Iyengar, and Naveen Kumar Chaudhary. 2024. Securing the future: advanced encryption for quantum-safe video transmission. *IEEE Transactions on Consumer Electronics* (2024).

[17] Yashas Hariprasad, SS Iyengar, and N Subramanian. 2024. Deepfake video detection using lip region analysis with advanced artificial intelligence based anomaly detection technique. *Authorea Preprints* (2024).

[18] Yashas Hariprasad, KJ Latesh Kumar, L Suraj, and SS Iyengar. 2022. Boundary-based fake face anomaly detection in videos using recurrent neural networks. In *Proceedings of SAI Intelligent Systems Conference*. Springer, 155–169.

[19] SS Iyengar, Seyedsina Nabavirazavi, Yashas Hariprasad, Prasad HB, and C Krishna Mohan. 2025. Artificial Intelligence in Practice: Theory and Application for Cyber Security and Forensics.

[20] SS Iyengar, Seyedsina Nabavirazavi, Yashas Hariprasad, Prasad HB, and C Krishna Mohan. 2025. Temporal Deepfake Generation and Detection in Video Sequences Using Recurrent Neural Networks (RNNs). In *Artificial Intelligence in Practice: Theory and Application for Cyber Security and Forensics*. Springer, 309–334.

[21] Eshaq Jamdar and Amith Kamath Belman. 2025. SyntheticPop: Attacking Speaker Verification Systems With Synthetic VoicePops. *arXiv preprint arXiv:2502.09553* (2025).

[22] Lily Lee and W Eric L Grimson. 2002. Gait analysis for recognition and classification. In *Proceedings of Fifth IEEE International Conference on Automatic Face Gesture Recognition*. IEEE, 155–162.

[23] Jani Mantyjarvi, Mikko Lindholm, Elena Vildjiounaite, S-M Makela, and HA Ailisto. 2005. Identifying users of portable devices from gait pattern with accelerometers. In *Proceedings.(ICASSP'05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005.*, Vol. 2. IEEE, ii–973.

[24] Hafiz Farhan Maqbool, Muhammad Afif Bin Husman, Mohammed I Awad, Alireza Abouhossein, Nadeem Iqbal, and Abbas A Dehghani-Sanij. 2016. A real-time gait event detection for lower limb prosthesis control and evaluation. *IEEE transactions on neural systems and rehabilitation engineering* 25, 9 (2016), 1500–1509.

[25] Mpho P Mufandaidza, Tshepiso D Ramotsoela, and Gerhard P Hancke. 2018. Continuous user authentication in smartphones using gait analysis. In *IECON 2018-44th Annual Conference of the IEEE Industrial electronics society*. IEEE, 4656–4661.

[26] Donald A Neumann and Elisabeth Roen Kelly. 2010. Kinesiology of the musculoskeletal system: foundations for rehabilitation. (2010).

[27] Claudia Nickel. 2012. Accelerometer-based biometric gait recognition for authentication on smartphones. (2012).

[28] Liu Rong, Duan Zhiguo, Zhou Jianzhong, and Liu Ming. 2007. Identification of individual walking patterns using gait acceleration. In *2007 1st international conference on bioinformatics and biomedical engineering*. IEEE, 543–546.

[29] Bin Shi and Sundararaja S Iyengar. 2020. *Mathematical theories of machine learning-Theory and applications.* Springer.

[30] Jayakumar Singaram, SS Iyengar, and Azad M Madni. 2023. Deployment of Deep Learning Networks. In *Deep Learning Networks: Design, Development and Deployment.* Springer, 99–134.

[31] Jayesh Soni, Subhash Gurappa, and Himanshu Upadhyay. 2024. A Comparative Study of Deep Learning Models for Image Super-Resolution Across Various Magnification Levels. In *2024 IEEE International Conference on Future Machine Learning and Data Science (FMLDS).* IEEE, 395–400.

[32] Hoang Minh Thang, Vo Quang Viet, Nguyen Dinh Thuc, and Deokjai Choi. 2012. Gait identification using accelerometer on mobile phone. In *2012 International Conference on Control, Automation and Information Sciences (ICCAIS)*. IEEE, 344–348.

[33] Changsheng Wan, Li Wang, and Vir V Phoha. 2018. A survey on gait recognition. *ACM Computing Surveys (CSUR)* 51, 5 (2018), 1–35.

[34] Johny Xiong and Amith Kamath Belman. 2025. Multi-Modal Adversarial Activity Detection Using Keyboard and Mouse Dynamics. In *2025 IEEE World AI IoT Congress (AIIoT)*. IEEE, 0340–0345.

[35] Min Zhang. 2019. Gait activity authentication using LSTM neural networks with smartphone sensors. In *2019 15th international conference on mobile Ad-Hoc and sensor networks (MSN)*. IEEE, 456–461.

[36] Tiantian Zhu, Lei Fu, Qiang Liu, Zi Lin, Yan Chen, and Tieming Chen. 2020. One cycle attack: Fool sensor-based personal gait authentication with clustering. *IEEE Transactions on Information Forensics and Security* 16 (2020), 553–568.

Received XX; revised XX; accepted XX