Active Attack that Exploits Biometric Similarity Difference and Basic Countermeasures

Pin Lyu[1], Wandong Cai[1], and Yao Wang[2(✉)]

[1] Northwestern Polytechnical University, Xi'an 710129, China
lvpin@mail.nwpu.edu.cn, caiwd@nwpu.edu.cn
[2] Xidian University, Xi'an 710126, China
wangyao@xidian.edu.cn

Abstract. As one of the most popular IoT (Internet of Things) devices, smartphone stores sensitive personal information. As a result, authentication on smartphones attracts widespread attention in recent years. Sensor-based authentication methods have achieved excellent results due to their feasibility and high efficiency. However, the current work lacks comprehensive security verification, undetected potential vulnerabilities are likely to be leveraged to launch attacks on these authentication approaches. We propose a novel attack to evaluate the reliability and robustness of the existing authentication methods. The basic idea behind our strategy is that the system has its authentication error; we elaborately analyze the false-negative samples to summarize its vulnerable properties and leverage such vulnerabilities to design our attack. The experiment result proves the feasibility of our attack and also demonstrates the drawbacks of the existing approaches. In addition, we propose a corresponding protect approach to defend against this attack, of which the scheme has the self-learning ability to update according to the newly detected attacks. Compared with authentications using multiple sensors, we only adopt a single accelerometer to achieve an EER of 5.3%, showing the convenience and effectiveness of our system.

Keywords: Gait authentication · Wearable sensors · Impersonation attack

1 Introduction

Biometric authentication combines computer and optical, acoustic, biosensor, and biostatistical principles using the human body's inherent physiological characteristics (e.g., fingerprints, faces, and irises) and behavioral features (e.g., handwriting, voice, and gait) to identify individuals. It provides both convenience and security for mobile device users, leading to biometric authentication

Supported by the National Natural Science Foundation of China (Grant No. 62002278).

W. Bao et al. (Eds.): ADHOCNETS 2021/TridentCom 2021, LNICST 428, pp. 81–95, 2022.
https://doi.org/10.1007/978-3-030-98005-4_7

being the most prevalent authentication method. With the development of IoT devices, there are more and more built-in sensors in smartphones, including many biometric sensors. Users can use smartphones to implement more authentication schemes, these methods can be authenticated without the user's knowledge and added to the security systems to determine the legitimate users. One of the actual implementations is gait recognition, which has matured in recent years to become a low-cost and reliable method for authenticating users [1,2].

Although biometric-based authentication systems can balance security and usability, they also face many security threats. Playback attacks and imitation attacks are more efficient and less disruptive to the system in terms of complexity and efficiency of implementation [3]. They affect the authentication process and difficult for the system to detect. In contrast, in the scenario of an imitation attack, the attacker has the same status as the victim when facing authentication systems. The available resources and knowledge about victims can directly affect the complexity of an attack on a biometric system. However, unlike other biometric features, the various data related to gait can be collected in public. In addition, applications [4–9] based on biometric uniqueness are increasing, so it is essential to ensure the robustness [2,4,10–12] of the authentication system.

We designed an attack plan, training 20 participants with similar physical conditions using the same gait, and conducted training lasting four months. This work complements the part about the failure to complete the zero-effort and minimum-effort attacks in mimic attacks [1]. Then, we used the existing gait recognition scheme as a target system and analyzed the results to study the reasons behind underperformance.

We propose a new algorithm by studying feature loss, long-time training, and muscle memory. We use the direction of force lost in calculating the acceleration value to calculate the similarity. This process does not require the use of new sensors or equipment. The experimental results show that our method performs better than the multi-device multi-sensor solution. Furthermore, it is stable in multiple scenes.

2 Related Work

Human gait refers to a manner of walking, stepping, or running [13]. Kinetic studies and clinical studies on gait systems began in the 1950s. Gait is universal uniqueness [14], and according to that, we can extract gait features during walking, and after classification and recognition, they can finally achieve the purpose of authentication or recognition.

2.1 Attack Models of Behavioral Biometric Traits

An attack on a biometric system challenges the uniqueness of a person's behavioral biometric traits. A.K. Jain divided the attacks that can compromise the security provided by the system into two basic types:

Zero-Effort or Passive Attacks. The identification system uses biometric features to distinguish people. When there is a fundamental similarity between the attacker and victim's features, it will cause a false match (FM).

Adversary or Active Attacks. An attacker actively impersonates a legitimate user through knowledge about the victim and the biometric system. The attacker can spoof the identity system by using digital or physical artifacts with the victim's characteristics.

2.2 Gait Recognition for Authentication

In 2005, Ailisto et al. [15] published their research on using a WS-based approach for gait analysis. It is the first work in this area to our knowledge. After that, researchers used many kinds of motion sensors [16–18] for collecting the motion of specific body parts. Studies by Gafurov [19] show that different human limb movements have different degrees of uniqueness and universality. Nowadays, smartphones have many built-in sensors, such as accelerometers, gyroscopes, and magnetometers. Gait analysis based on dedicated wearable sensors made it possible to use the smartphones' built-in sensors for authentication. Since2009, smartphone-based gait authentication has become a hot research area, and many researchers have made significant contributions [1,20–24]. With the popularization of devices such as smartwatches and sports bracelets in recent years, authentication schemes that combine multiple devices have gradually emerged [2,4].

2.3 Impersonation Attacks

Although human gait is unique, the detection system is often not perfect, so many researchers are keen to design various imitation attacks to break through the existing authentication system.

In Stang's work [25], 13 students volunteered to contribute to his experiment. During the imitation process, the attackers did not see the victims' gaits, but only a simple description displayed on a big screen. The drawback in Stang's work is the experimental environments, too few data points can hardly form a curve, sample rate as low as 30, and 5 s is too short of making the gait from start to natural.

Gafurov et al.'s experiment [26] divided the attackers into two parts: the "friendly" scenario and the "hostile" scenario. In the former scenario, participants walked naturally in their styles, while participants tried to imitate their partners in the latter scenario. A dedicated sensor was attached to the belt around the right hip. Gafurov et al.'s results indicated that the chances of accepting impostors employing a minimal effort, mimicking the "hostile" scenario, is not higher than the chances of impostors succeeding in the "friendly" scenario.

Based on the work of predecessors, Mjalaand et al. [27] divided their experiment into three scenarios: friendly, short-term hostile, and long-term hostile. In the friendly scenario, they selected one victim and six attackers from participants. The selected victims had visible gait characteristics that made the

imitation process more accessible, and the victim's gait is steady to suffer psychological and outside influence. The attackers who were close in height to the victims were selected. This research using belt attachment. Muaaz [1] pointed out that watching a video or looking at a walking data chart obscures many details of the target.

In Muaaz's study [1], the chosen five attackers were acting students trained as mime artists, specializing in mimicking body motions and body language. Like previous studies [26,27], in 29% of impersonation attempts, attackers lost regularity while mimicking the victim.

Rajesh Kumar et al. [28] and Babins Shrestha et al. [2] used digital treadmills to train attackers. Although the attacker has a sample of the victim's gait pattern in this attack, the attacker does not imitate it. They use a treadmill to restrict the attacker's gait features, such as speed, step length, stride length, and match the features extracted from the victim's walking pattern.

In summary, there are already excellent solutions in the scenario of zero-effort attack, and the scenario of active attack requires us to focus. So when designing a gait authentication system, the following criteria must be considered:

1. Robust: The system needs to resist the attacker's mimic attacks and passive attacks in different scenarios.
2. Fast: Based on ensuring precision and recall rate, perform faster authentication.
3. Lightweight: Based on ensuring accuracy, minimize resource consumption, including memory consumption and power consumption due to calculation.

3 Design and Implementation of Attack

The rationale of biometric systems is using the uniqueness of physiological features to resist attacks. However, in the actual scenario, if the features cannot distinguish between the attacker and the legitimate user, the attacker will be authorized. For a lightweight system, the attacker can not pass authentication is the essential requirement; the victim's performance can be much better than the "Same" evaluation.

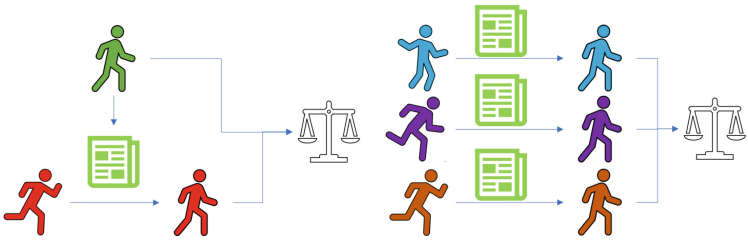
3.1 Our Motivation

Our attack mode inspired by Cauchy sequence (Eq. 1) in math: A sequence $\{x_i\}$ of elements in a metric space $\{X, d\}$ such that for any $\varepsilon > 0$ there is a number N such that:

$$d(x_n, x_m) < \varepsilon \qquad \forall m, n \geq N \tag{1}$$

In a successful impersonation attack of the gait authentication system, the attacker's performance can get the "Same" evaluation of the system. Since the legal user's performance is on the "Same" side, at least two different people will get the system's "Legal" evaluation in a successful attack. That leads to

our attack: in the evaluation function of an authentication system, make the performance of at least two users as similar as possible and get the "Legal" evaluation. Base on the theory above, we suppose to use one action specification to train the participants and then detect whether the system can separate each other.



(a) Imitation Attack (b) Our Attack

Fig. 1. Imitation attack and our attack

As shown in Fig. 1, we do not use the imitation method of Fig. 1a but use Fig. 1b to implement our attack. We use the same action method to train all participants and then use their gait after training to make comparisons. Increased FAR or incorrect authorization will indicate the effectiveness of our attack. Our attack scheme has performed well on some systems, and we will discuss this result in later chapters. Besides, the training method designed in this way can well avoid the "wolves" (better imitators) and "sheep" (more likely to be imitated) problem [29] among the participants. Using uniform movement specifications and participants' are similar in size, which made "sheep" cannot exist. Furthermore, the participants' training time is long enough, and they formed muscle memory of the gait; in this situation, the advantages of "wolf" are also no longer apparent.

3.2 Participant Demographics

We invite 20 young men who will participate in the selection of honor guards to join our research. Before being invited, they had at least three months of military training and four months of Goose-step training which experience allowed them to persevere in our training program. Since the selection qualifications include body values, which provides great convenience for our research, the values of our participates are similar: all participants were male and of similar age, height, weight.

3.3 Training Instructions

Before participating in our research, the participants have gone through quite a long goose-step training. We combined the goose-step with the gait of ordinary people to design our walk style.

We train the participants of this gait for one hour a day for three months. Participants are required to walk every day in this style. In addition to daily individual training, they also train together every Sunday. Besides, we asked participants to walk in a queue when meeting other participants in daily life. The primary purpose of this training method is to build muscle memory of the training gait to avoid the problems of improvisation and irregular in the previous studies [1].

3.4 Performance of Our Attack on Previous Method

To examine the effectiveness of the attack we designed, we implement Muaaz's method [1] as the evaluation standards.

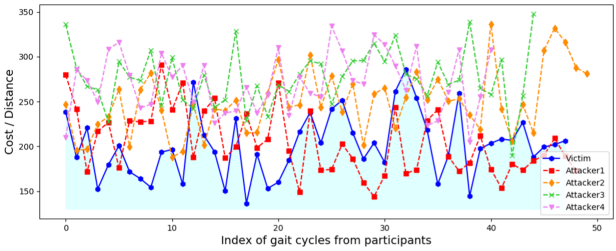


Fig. 2. Our attack on the existing system.

Figure 2 shows our attack effects in the existing scenario. The horizontal axis is the gait period arranged in chronological order, and the vertical axis is the distance between the gait and the template. The polyline represents the DTW distance (or cost) between the participants and the victim's gait template. The blue one is the evaluation of the victim; the other four polylines represent the best four attackers' performance. The smaller the distance, the higher the similarity with the victim. It can be seen from Fig. 2 that it is difficult to find a value as a threshold to distinguishing attackers and the victim.

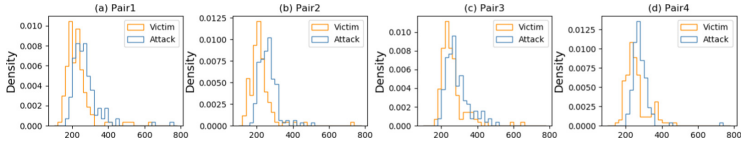


Fig. 3. Distribution of the best four attacker-victim pairs when using acceleration values to calculate DTW distance.

Figure 3 shows the distributions of DTW distance of the four attacker-victim pairs in all attempts. In the figure, the horizontal axis represents the DTW distance of the participant's gait and the template, and the vertical axis represents the distribution density. From the figure, we observe that the attackers' data are similar to the victims'.

Obviously, after a training period, the previous gait recognition system based on acceleration values did not distinguish between attackers and a victim by using a threshold; in other words, our attack can confuse the system to produce misjudgment.

3.5 Reasons Behind Underperformance

According to the performance of our attack, we need to study the reasons behind the result.

Muscle Memory. All the participants in our study formed muscle memory of the gait through long-term training. Thus all the participants can avoid the problems of improvisation and irregularity found in previous work [1]. We can see the results from Fig. 2 and Fig. 3, which show that participants have stable performance. Furthermore, the result shows that the gait we designed has become participants' own.

Detailed Instructions. The gait details used in training are all quantified, and the training process includes single training and collective training, which avoids mutual compromise during joint training [30,31].

Feature Loss. The raw data obtained from the accelerometer is the acceleration in three directions of the mobile phone are three vectors ($a_x(t)$,$a_y(t)$,$a_z(t)$). In calculating the acceleration value (see Eq. 2), lost the characteristic of the direction, and finally, only a scalar ($A(t)$), acceleration value, is remained. Therefore, it will be vulnerable when only relying on one feature to deal with our attacks.

$$A(t) = \sqrt{a_x^2(t) + a_y^2(t) + a_z^2(t)} \tag{2}$$

4 Our Authentication Approach

In this section, we introduce our system and its components and algorithm.

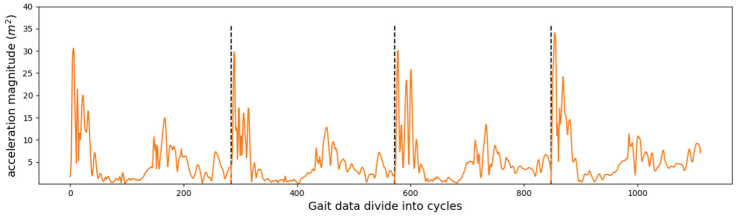
4.1 Approach Overview

Our goal is that the system can authorize attackers who have been trained together with legitimate users for a long time under the same instruction. In addition, we also need to minimize the use of resources while meeting the essential authentication functions. After many attempts, we use the changing of the force in walking as the feature of our study. Thus we use the data collected by the accelerometer to construct an authentication scheme.

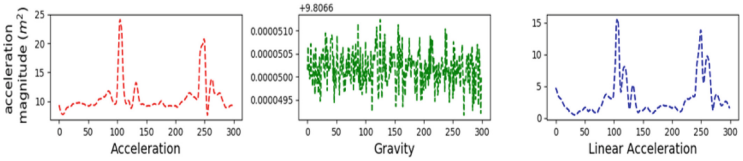
We first preprocess the obtained raw data and then divide it into gait cycles. After aligning the coordinate system, we calculate the distance between the current user's gait from the victim's template, and we use spherical radian as the distance unit in the calculation. Finally, using the evaluation system to decide whether to authorize the current user.

4.2 Data Preprocessing

The primary function of data preprocessing is to convert the raw data into usable gait cycles.



(a) Gait Cycles



(b) Filter Gravity

Fig. 4. Data preprocessing

Walking Data Extraction. Since the start time of the gait data record is earlier than the start time of the walk, and the end time is later than the end time of the walk, it is necessary to remove the non-walking phase data. In our study, we used 250 sample points as a sliding window. When the value of acceleration exceeds the threshold (the default value is 16) for five consecutive windows, it indicates that these windows are in the walking phase.

S-G Filter. Raw data contains random noise, and we used S-G [32] filters (as in (3)) to filter out significant portions of the high-frequency content and noise and minimize the error while maintaining waveform and height. As shown in formula 3, $X \cdot \left(X^T \cdot X\right)^{-1} \cdot X^T$ is the convolution coefficient, Y is the observation value, and Y' is the smoothing result.

$$Y' = X \cdot \left(X^T \cdot X\right)^{-1} \cdot X^T \cdot Y \tag{3}$$

Cycle Extraction. We took 200 consecutive sample points from the middle of the data as a sliding window and then slid back in steps of 1 to get a series of data sets containing 200 sample points. The sums of the Euclidean distances of each point set and the corresponding point in the first window were calculated, finally yielding a distance sequence. The distance between the local minimums is the length of the cycle, and then the number of sample points per cycle is averaged.

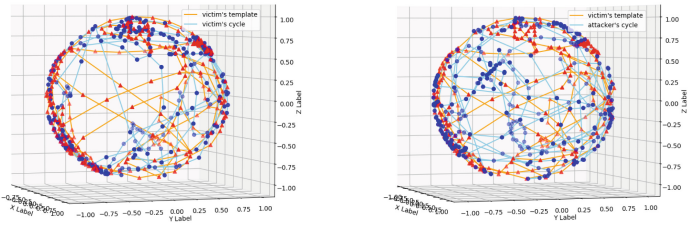
After finding the length of one cycle, we began to divide the data set into separate cycles. We used 1.5 times the cycle length of the interval to detect the local minimum. When obtain a minimum value, starting from the index of that point, we created a new interval (length of 1.5 times the cycle length) forward. We searched the local minimum from the vicinity of a cycle length position within this interval. The use of 1.5 times the period as the interval length is due to the uncertainty of the gait. Although there is always a deviation in the interval length of each step, the deviation will not be too large (see Fig. 4a).

Gravity Separation. During walking, the direction of gravity relative to the smartphone's coordinate is constantly changing. Since the value is too significant (approximately $9.8\,\mathrm{m/s^2}$) to ignore, we need to eliminate the contribution of the force of gravity. From the built-in filter in Android, we can obtain linear acceleration through the function $Sensor.TYPE\_ACCELEROMETER$.

Abnormal Cycles Removal. Occasionally, some accidental situations caused data anomalies during walking, and we needed to remove the abnormal cycles. We used DTW (dynamic time warping) to determine the degree of dispersion of the cycles and cross-compare the DTW distances between different cycles. We removed cycle pairs that had a significant deviation from the distance.

4.3 Coordinate Aligning

In order to assess whether the direction of the force can be used as a feature to identify the movement of the people's gait, we made a simple comparison. Figure 5 show the differences of direction in a gait cycle between victims alone and victims with attackers. From this, we can see that based on the victim's gait template (red triangle and orange line), the attacker's performance (see Fig. 5b) is more chaotic than the victim (see Fig. 5a). Therefore, we believe that we can use the force direction as an essential feature for identity verification.



(a) Comparison of the two gait cycles of the victim

(b) Comparison of the gait cycle of victim and attacker

Fig. 5. Differences in the direction of acceleration

According to the distribution characteristics of Fig. 5, we need to rotate the coordinate system of the gait data obtained in the certification process to make it conform to the coordinate system of the template.

Direction Extraction
Acceleration is a vector with magnitude (or length) and direction. We determined the magnitude *A(t)* from (2) in Sect. 4.2. Therefore, we can obtain the direction on the three axes:

$$d_x = \frac{a_x}{A(t)},\ d_y = \frac{a_y}{A(t)},\ d_z = \frac{a_z}{A(t)} \tag{4}$$

Using (4), the acceleration can be changed into a unit vector with length 1. Applying this method to the gait data, we will get a sequence of ordered point sets distributed over a unit sphere. Each point represents the direction of acceleration, that is, the direction of the force at that time.

Distance Between Cycles
The shortest path between two points on a sphere, also known as an orthodrome, is a segment of a Great-Circle. The spherical distance can be measured using arc length, which is the angle between two points in polar coordinates. We can use the inner vector product to calculate the angle:

$$\cos(\theta) = \frac{\vec{a} \cdot \vec{b}}{|\vec{a}| \left|\vec{b}\right|} \tag{5}$$

In (5), the lengths of vectors are 1, so the distance between the two points is:

$$dist(a, b) = \theta = \arccos\left(\vec{a} \cdot \vec{b}\right) \tag{6}$$

In addition, according to our statistical results, the angle between two adjacent points is between 0 and 0.5π, because based on our sampling rate, no one can swing his or her leg more than 90° in such a short time.

$$D(i, j) = dist(i, j) + min \begin{cases} D(i-1, j) \\ D(i, j-1) \\ D(i-1, j-1) \end{cases} \tag{7}$$

We used the formula (as in (7)) to calculate the distance between cycles. The calculation is using in the template creation phase and the authentication phase. A shorter distance means more similar to the template. If the distance is below a certain level, we will decide on the success of the authentication.

Finally, we cross-compare the cycles and calculate the distance. We use the KNN (k-Nearest Neighbor) algorithm to determine which cycles to submit for the system. If it is in the registration phase, the submitted cycles using as legal user's template; the distance will be saved for the authentication function to get the threshold. If it is in the verification phase, the system using it to calculate

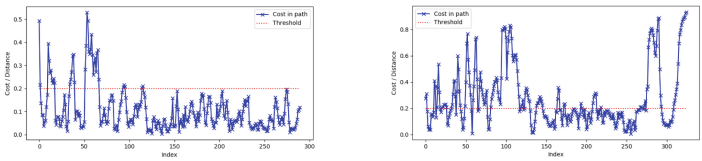
the distance. We will drop it for the cycles that the distance is far from the current template (the default distance is 450).

Coordinate System Alignment

Before comparison, we need to align the coordinate system of the new data with the template. We will reposition the phone before the data collection each time, causing the offset in the position and the twist of the orientation.

In $p = [0, \mathbf{p}]$, we can represent a three-dimensional vector as a pure quaternion. In $q = \left[\cos\frac{1}{2}\theta, \sin\frac{1}{2}\theta\hat{\mathbf{v}}\right]$, we use a rotation quaternion to represent the rotation, where $\hat{v}$ represents the axis of rotation and θ represents the angle of rotation around $\hat{v}$. Finally, using (8), we can get the vector p' after vector p is rotated by the quaternion q.

$$p' = qpq^{-1} \tag{8}$$



(a) Distribution of distance of victim's two cycles

(b) Distribution of distance of victim and attacker

Fig. 6. Differences in the distribution of cycles

According to Fig. 6, for different participants, the distance in a cycle in the middle part is significantly shorter than the remaining part (most of the points is less than o.2). Therefore, we use that part to calculate the quaternion, then use the entire cycle to get the distance.

Using the Lagrange multiplier to calculating the shortest distance, we can obtain the quaternion required to rotate the coordinate system. The quaternion represents the rotation and then applies to other data cycles. At last, we are using the rotated cycles to calculate the similarity.

4.4 Similarity Comparison

As mentioned in Sect. 4.3, we measure the distance between the current user's live template and the saved template. When the distance is below the threshold, return the confidence score (the maximum value is 100%). If the confidence score exceeds 50%, we consider the current user (and the user in the template) to be "Same."

5 Performance and Discussion

Our experiment uses two OPPO-R9s, two MI8s, and one MI8 SE as devices to collect gait data; twenty participants (mentioned in Sect. 3.2). We installed the app on the devices and then saved the calculation results and the original data separately and recorded the timestamps for future research. When collecting data, participants place the smartphone in the front right pocket of the trousers. Moreover, participants must walk for at least 1 min in the trained gait. The detection error tradeoff (DET) curve, which represents the performance based on our approach (given in Sect. 4)'s false match rate (FMR) and false non-match rate (FNMR) errors. Finally, we achieved an EER of 5.3%.

5.1 Performance of Our Approach

Since the attacker does not need to imitate a specific victim in our scheme, we can select the best-performing attacker-victim pair for evaluation. Figure 7 shows the confidence scores of the best-performing attacker-victim pairs for authentication.

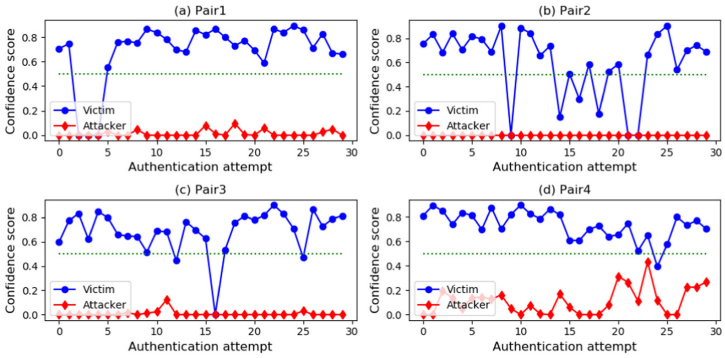


Fig. 7. Best-performing attacker-victim pairs.

Figure 7 shows the confidence scores of the best-performing attacker-victim pairs for authentication. The results show that no attacks were successful; that is to say, our scheme can resist our attacks. However, in the 6% scenario, the victim did not pass the verification of his template. We checked the timestamp and found that most of this event occurred at the end of the walk, and the confidence scores of the victims would fluctuate greatly. When we extended the walking time, the appearance of this phenomenon was delayed. One possible reason is that when the walk is nearing the end, the participants' attention will shift to other aspects, such as waiting for a stop signal or preparing to take out the device, thus losing the stability of their gaits. At this stage, the real-time scores of the victim and the attacker also cause large fluctuations.

In addition, we analyzed the original data sequence and found that 1.7% of attacks were successful in the best-performing victim-attacker pair. The peak of confidence reached 54.1%, but this data was abandoned during the data preprocessing (Sect. 4.3) and failed to enter the authentication phase.

5.2 Performance Under Different Gait

As mentioned in Sect. 3.2, we recruited 20 participants. We collected three different gait data from them (gait of their own, our trained style, and the goose style). We collected ten sets of data for each participant's gait and finally divided them into about 1200 samples (for each gait). We use 10-fold cross-validation to measure the performance of participants. Compared with the previous multi-sensor authentication system using random forest, our results have similar precision and recall rates.

Table 1. Result of our approach

	FNR	FPR	Recall	Precision	F1-score
Goose step	0.093	0.092	0.907	0.907	0.907
Training style	0.077	0.082	0.918	0.922	0.920
Own style	0.054	0.053	0.945	0.946	0.945

6 Conclusion

Research in the field of mobile-based biometrics is continuing. In our work, we propose and implement a novel attack scheme to evaluate the reliability of the gait recognition scheme. We designed and implemented an Android application to record the user's exercise data. Although a human can not imitate other's gait, we have proved that it is possible to successfully attack specific gait verification systems. Based on that, we propose a new gait authentication scheme to defend against this attack and to upgrade our application. In the attack scenario, we achieved an EER of 5.3%. Moreover, it achieved the same precision and recall rate as the verification scheme [2] using multiple devices and machine learning algorithms. Although the data used in the attack scenario only contains a few topics, the results of this study complement previous work [1] and prove that high-intensity training can increase the attacker's chances of passing the verification system. We believe that there is a decline in similarity in training to imitate (the attacker loses the regularity of his pace while imitating the victim). After that, it rises (muscle memory formed as the gait becomes natural).

In future work, we want to solve some related problems. We want to infer some physical information of the phone holder based on the acceleration data. Moreover, we want to know how long it takes to learn and adapt to a new gait to pass specific gait verification systems. We can study these issues as information security topics.

References

1. Muaaz, M., Mayrhofer, R.: Smartphone-based gait recognition: from authentication to imitation. IEEE Trans. Mobile Comput. **16**(11), 3209–3221 (2017). https://doi.org/10.1109/TMC.2017.2686855, http://ieeexplore.ieee.org/document/7885511/
2. Shrestha, B., Mohamed, M., Saxena, N.: Zemfa: zero-effort multi-factor authentication based on multi-modal gait biometrics. In: 2019 17th International Conference on Privacy, Security and Trust (PST), pp. 1–10 (2019)
3. Ratha, N.K., Connell, J.H., Bolle, R.M.: An analysis of minutiae matching strength. In: Bigun, J., Smeraldi, F. (eds.) AVBPA 2001. LNCS, vol. 2091, pp. 223–228. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45344-X_32
4. Brüsch, A., Nguyen, N., Schürmann, D., Sigg, S., Wolf, L.: Security properties of gait for mobile device pairing. IEEE Trans. Mobile Comput. **19**(3), 697–710 (2020). https://doi.org/10.1109/TMC.2019.2897933
5. Revadigar, G., Javali, C., Xu, W., Vasilakos, A.V., Hu, W., Jha, S.: Accelerometer and fuzzy vault-based secure group key generation and sharing protocol for smart wearables. IEEE Trans. Inf. Forensics Secur. **12**(10), 2467–2482 (2017). https://doi.org/10.1109/TIFS.2017.2708690
6. Nandakumar, K., Jain, A.K., Pankanti, S.: Fingerprint-based fuzzy vault: implementation and performance. IEEE Trans. Inf. Forensics Secur. **2**(4), 744–757 (2007). https://doi.org/10.1109/TIFS.2007.908165
7. Nandakumar, K., Jain, A.K.: Multibiometric template security using fuzzy vault. In: 2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems, pp. 1–6, September 2008. https://doi.org/10.1109/BTAS.2008.4699352
8. Zhang, Z., Wang, H., Vasilakos, A.V., Fang, H.: ECG-cryptography and authentication in body area networks. IEEE Trans. Inf. Technol. Biomed. **16**(6), 1070–1078 (2012). https://doi.org/10.1109/TITB.2012.2206115
9. Venkatasubramanian, K.K., Banerjee, A., Gupta, S.K.S.: PSKA usable and secure key agreement scheme for body area networks. IEEE Trans. Inf. Technol. Biomed. **14**(1), 60–68 (2010). https://doi.org/10.1109/TITB.2009.2037617
10. Hoang, T., Choi, D.: Secure and privacy enhanced gait authentication on smart phone. Sci. World J. **2014** (2014)
11. Mjaaland, B.B.: Gait mimicking: attack resistance testing of gait authentication systems. Master's thesis, Institutt for telematikk (2009)
12. Liu, L.-F., Jia, W., Zhu, Y.-H.: Survey of gait recognition. In: Huang, D.-S., Jo, K.-H., Lee, H.-H., Kang, H.-J., Bevilacqua, V. (eds.) ICIC 2009. LNCS (LNAI), vol. 5755, pp. 652–659. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-04020-7_70
13. Dictionary.com: Gait — define gait at dictionary.com. https://www.dictionary.com/browse/gait. Accessed 1 Oct 2018
14. Murray, M.P.: Gait as a total pattern of movement: including a bibliography on gait. Am. J. Phys. Med. Rehabil. **46**(1), 290–333 (1967)
15. Ailisto, H.J., Lindholm, M., Mantyjarvi, J., Vildjiounaite, E., Makela, S.M.: Identifying people from gait pattern with accelerometers. In: Biometric Technology for Human Identification II. vol. 5779, pp. 7–15. International Society for Optics and Photonics (2005)
16. Jin, R., Shi, L., Zeng, K., Pande, A., Mohapatra, P.: Magpairing: pairing smartphones in close proximity using magnetometers. IEEE Trans. Inf. Forensics Secur. **11**(6), 1306–1320 (2015)

17. Morris, S.J.: A shoe-integrated sensor system for wireless gait analysis and real-time therapeutic feedback. Ph.D. thesis, Massachusetts Institute of Technology (2004)
18. Huang, B., Chen, M., Huang, P., Xu, Y.: Gait modeling for human identification. In: Proceedings 2007 IEEE International Conference on Robotics and Automation, pp. 4833–4838, April 2007. https://doi.org/10.1109/ROBOT.2007.364224
19. Gafurov, D.: A survey of biometric gait recognition: approaches, security and challenges. In: Annual Norwegian Computer Science Conference, pp. 19–21 (2007)
20. Heinz, E.A., Kunze, K.S., Sulistyo, S., Junker, H., Lukowicz, P., Tröster, G.: Experimental evaluation of variations in primary features used for accelerometric context recognition. In: Aarts, E., Collier, R.W., van Loenen, E., de Ruyter, B. (eds.) EUSAI 2003. LNCS, vol. 2875, pp. 252–263. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-39863-9_19
21. Sprager, S., Zazula, D.: A cumulant-based method for gait identification using accelerometer data with principal component analysis and support vector machine. WSEAS Trans. Signal Process. **5**(11), 369–378 (2009)
22. Kwapisz, J.R., Weiss, G.M., Moore, S.A.: Cell phone-based biometric identification. In: 2010 Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), pp. 1–7. IEEE (2010)
23. Nickel, C.: Accelerometer-based biometric gait recognition for authentication on smartphones. Ph.D. thesis, Technische Universität (2012)
24. Zhong, Y., Deng, Y., Meltzner, G.: Pace independent mobile gait biometrics. In: 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), pp. 1–8. IEEE (2015)
25. Stang, Ø.: Gait analysis: is it easy to learn to walk like someone else? Master's thesis (2007)
26. Gafurov, D., Snekkenes, E., Bours, P.: Spoof attacks on gait authentication system. IEEE Trans. Inf. Forensics Secur. **2**(3), 491–502 (2007). https://doi.org/10.1109/TIFS.2007.902030
27. Mjaaland, B.B., Bours, P., Gligoroski, D.: Walk the walk: attacking gait biometrics by imitation. In: Burmester, M., Tsudik, G., Magliveras, S., Ilić, I. (eds.) ISC 2010. LNCS, vol. 6531, pp. 361–380. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-18178-8_31
28. Kumar, R., Phoha, V.V., Jain, A.: Treadmill attack on gait-based authentication systems. In: 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), pp. 1–7 (2015)
29. Mjaaland, B.B.: The plateau: imitation attack resistance of gait biometrics. In: IFIP Working Conference on Policies and Research in Identity Management. pp. 100–112. Springer, Berlin (2010). https://doi.org/10.1007/978-3-642-37282-7
30. Fernandez-Lopez, P., Sanchez-Casanova, J., Liu-Jimenez, J., Morcillo-Marin, C.: Influence of walking in groups in gait recognition. In: 2017 International Carnahan Conference on Security Technology (ICCST), pp. 1–6, October 2017. https://doi.org/10.1109/CCST.2017.8167842
31. Fernandez-Lopez, P., Kiyokawa, K., Wu, Y., Liu-Jimenez, J.: Influence of walking speed and smartphone position on gait recognition. In: 2018 International Carnahan Conference on Security Technology (ICCST), pp. 1–5 (2018). https://doi.org/10.1109/CCST.2018.8585427
32. Anwary, A.R., Yu, H., Vassallo, M.: Optimal foot location for placing wearable IMU sensors and automatic feature extraction for gait analysis. IEEE Sens. J. **18**(6), 2555–2567 (2018). https://doi.org/10.1109/JSEN.2017.2786587