

Elevating Wearable Sensor Authentication with Hybrid Deep Learning and Squeeze-and-Excitation

Sakorn Mekruksavanich[1(✉)] and Anuchit Jitpattanakul[2]

[1] Department of Computer Engineering, School of Information and Communication Technology, University of Phayao, Phayao, Thailand
sakorn.me@up.ac.th

[2] Intelligent and Nonlinear Dynamic Innovations Research Center, Department of Mathematics, Faculty of Applied Science, King Mongkut's University of Technology North Bangkok, Bangkok, Thailand
anuchit.j@sci.kmutnb.ac.th

Abstract. Smartphones often contain users' private and sensitive information. Thus, continuous verification of identity is crucial to prevent unauthorized access. While sensor-based solutions have been explored before, recent advancements in machine learning have provided alternative deep-learning approaches for constantly checking if the smartphone's user is genuine. We put forward a hybrid deep convolutional neural network model named SE-DeepConvNet, which includes squeeze-and-excitation elements to improve representation learning from streams of smartphone sensor information. Using a benchmark human movement dataset, our experiments show state-of-the-art performance boosts with SE-DeepConvNet, realizing 99.78% accuracy and 0.38% equal error rate for user verification – surpassing other evaluated deep learning models. Our distinctive combination of the squeeze-and-excitation system and deep convolutional neural network framework enables optimized feature extraction from sequence information for accurate constant verification.

Keywords: Continuous authentication · Smartphone sensors · Squeeze-and-excitation module · Deep learning · Accurate continuous authentication

1 Introduction

Wearable devices like smartphones aim to bolster security through recurrent user identity verification using continuous authentication techniques. These methods can be broadly classified into two categories: those grounded in analyzing physiological biometrics and those centered around behavioral biometrics. Physiological techniques confirm static bodily attributes, encompassing facial patterns [8], fingerprints [28], Iris patterns [27], voice [3], and pulse [18]. In contrast, behavioral methods concentrate on identifying distinctive patterns in user interactions with

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2024
O. Gervasi et al. (Eds.): ICCSA 2024, LNCS 14814, pp. 186–197, 2024.
https://doi.org/10.1007/978-3-031-64608-9_12

the device over time [19]. Specifically, the former relies on unchanging physical traits, necessitating the user's direct involvement in the authentication process.

On the other hand, behavioral biometric approaches leverage patterns like touch gestures [37], gait [24], and GPS movements [4]. Extracting unique features from a user's natural interactions with the smartphone, these approaches gather data from various built-in components such as accelerometers, gyroscopes, magnetometers, and touch screens [20]. These methods implicitly model invariant user-specific traits by analyzing these multi-modal signals, eliminating the need for the user's active participation in the authentication process.

Continuous authentication has seen a surge in the adoption of gait recognition, primarily because of the unique walking patterns distinctive to each individual [2]. Techniques based on gait strive to automatically discern whether the current user of a wearable device is the rightful owner or an impersonator. This is accomplished by scrutinizing their motion signatures, extracted from the device's onboard motion sensors, and matching them against the owner's established profile. The fundamental concept here is to verify identity seamlessly by exploiting the individuality of one's walking gait compared to that of an imposter. If, during authentication checks, the deviations in the current user's gait surpass a predefined threshold, the system raises a flag indicating potential unauthorized access.

Gait analysis has recently been investigated for continuous authentication using wearable sensors [22]. Despite their convenience, current methods based on gait face limitations in accuracy, with many needing help to achieve authentication rates surpassing 95% and equal error rates between 5–10% [6]. To ensure reliable adoption, further research is essential to enhance accuracy. Recent advancements in deep learning for behavioral modeling provide promising alternatives to traditional manual feature engineering [26,29]. Deep neural networks can automatically learn representative features from sensor data, freeing us from the complexities of labor-intensive hand-crafted approaches. This enables the deployment of user authentication based on pervasive behaviors like gait captured through onboard sensors.

While deep learning has proven successful in classifying images and speech, its application to non-image/speech data, such as recognizing human behavior through raw sensor data, poses unique challenges. The presence of abundant noise in raw data introduces the risk of errors in behavior recognition during deep learning-based authentication. In addressing this issue, our work introduces a new deep learning model called SE-DeepConvNet, designed explicitly for continuous authentication based on sensor data. This model incorporates fully interactive layers by utilizing squeeze-and-excitation modules to tackle the challenges associated with continuous authentication. Experiments were conducted using the publicly available HMOG dataset to validate its effectiveness. The results of these experiments demonstrate that the proposed SE-DeepConvNet surpasses other baseline deep learning models, achieving higher accuracy and a lower equal error rate (EER).

The remainder of this article follows a structured outline. Recent related works are introduced in Sect. 2. Details about the SE-DeepConvNet model are outlined in Sect. 3. Our experimental results are presented in Sect. 4. Finally, Sect. 5 concludes this work and highlights challenging areas for future exploration.

2 Related Works

2.1 Continuous Authentication

Continuous authentication seeks to comprehend human behaviors, allowing computing systems to assist users proactively based on their needs. Human activities, like walking, sitting, working, and running, can be described as actions the user performs within a specific timeframe and protocol. Over the past decade, extensive research has been conducted on continuous authentication.

The growing number of sensors in standard mobile phones has directed attention towards gait features for authentication. Gait features are stable, distinguishable, and easy to collect but are also gaining significance due to people having their phones with them for longer durations. Additionally, there is a wealth of available gait features. An implicit authentication method based on gait identifies users by their walking style. Gait signal data from built-in sensors like accelerometers and gyroscopes can be easily accessed through mobile phones. By collecting these continuous data streams, discriminative gait features can be extracted and trained by a classifier for authentication. Various methods have been proposed for gait-based implicit authentication on mobile devices, differing primarily in how features are extracted from raw data or the authentication algorithm employed.

The study by Mantyjarvi et al. [17] employed methods utilizing correlation, frequency domain analysis, and data distribution statistics. Thang et al. [32] and Muaaz et al. [21] utilized the dynamic time warping method. Rather than relying on gait cycles for feature extraction, Nickel et al. [23] employed hidden Markov models for gait recognition. The mentioned methods require feature selection and extraction before user authentication, making these procedures intricate and laborious.

Zhong et al. [36] introduced a sensor direction-invariant gait representation called gait dynamic images. This method captures three-dimensional time series using a triaxial accelerometer, expressing GDI as the cosine similarity of the motion measurement at time t with the lag time signal. Damaševicius et al. [7] utilized random projections to reduce feature dimensionality to two, then computed the Jaccard distance between two probability-distributed functions of the derived features for identification. Kašys et al. [15] conducted user identity verification through a linear support vector machine (SVM) classifier on walking activity data captured by a mobile phone.

Xu et al. [34] introduced Gait-watch, a context-aware authentication system based on gait feature recognition and extraction during various walking activities. Abo El-Soud et al. [1] employed filter and wrapper approaches for

feature selection of gait data, utilizing a random forest classifier for authentication. Papavasileiou et al. [25] proposed GaitCode, a continuous authentication mechanism based on multi-modal gait-based sensor data. They used a network of auto-encoders with fusion for feature extraction and SVM for classification.

2.2 Deep Learning in Continuous Authentication

The realm of advanced learning [11] has showcased its effectiveness in domains connected to recognizing walking styles. This spans discerning actions [13], categorizing videos [14], and identifying faces [31]. Nevertheless, the training of advanced learning models demands copious data, posing a challenge due to the constraints in collecting abundant walking data, given the limitations in battery life and processing power of mobile devices. In comparison to conventional machine learning approaches, applications of advanced learning in problems related to implicit authentication through walking styles are relatively scarce.

Gadaleta et al. [9] introduced an authentication framework for users based on motion signals gathered from smartphones, labeled as IDNet. IDNet leverages convolutional neural networks (CNN) as versatile feature extractors, utilizing one-class SVM as a classifier. They directly input the original walking signal into the CNN, a method that is not ideal for CNNs as they are less adept at processing one-dimensional signals. Giorgi et al. [10] outlined an authentication framework for users, utilizing inertial sensors and incorporating recurrent neural networks (RNN) for deep learning-based classification. However, notable disparities were observed in results between known and unknown identities.

To enhance the effectiveness of deep learning approaches, cross-channel interaction presents evident advantages compared to recently suggested literature. Hu et al. [12] introduced a squeeze-and-excitation (SE) network to fine-tune channel feature responses. Chen et al. [5] employed channel-wise attention for tasks like semantic segmentation and image captioning. Wu and He [33] utilized group normalization, representing a specialized model with channel-wise communication.

However, the interactions across different channels in their models are overly simplistic, involving only the computation of mean and standard deviation of feature maps. In computer vision, Yang et al. [35] proposed cross-channel interaction at the same layer. This encourages communication among channels within the same layer, improving performance.

3 The Sensor-Based Continuous Authentication Framework

The continuous authentication system based on sensors utilized in our study encompasses four main phases:

1. Gathering raw data streams from sensors,
2. Pre-processing the signals to address missing values and eliminate noise,
3. Converting the refined signals into representative data instances,

4. Conducting supervised training and evaluation of machine learning models using the generated datasets.

This sequential processing pipeline facilitates the robust learning and assessment of authentication systems from sensor streams, illustrated in Fig. 1.

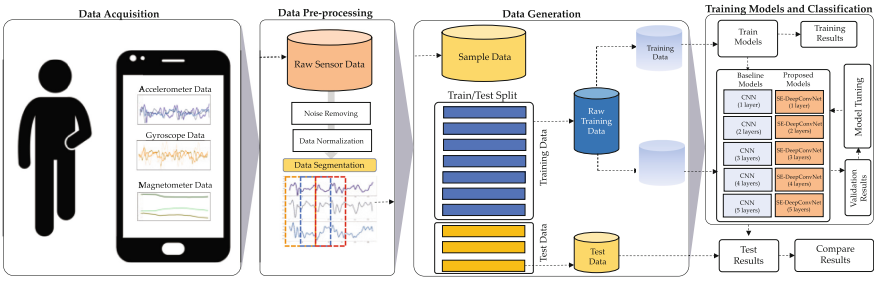

Fig. 1. The proposed framework of gait-based continuous authentication using wearable sensors.

3.1 HMOG Dataset

Experiments utilize the available HMOG smartphone sensor dataset to assess our proposed advanced learning approach, specifically designed for continuous authentication [30]. The HMOG dataset comprises readings from accelerometers and gyroscopes, gathered from 100 participants (53 male, 47 female) using 10 Samsung Galaxy S4 devices at a 100 Hz sampling rate. The participants engaged in sessions lasting 2-6 h, involving activities like reading documents, typing, and navigating maps. However, HMOG encounters challenges such as data gaps and aberrant readings for certain participants [16]. Consequently, we excluded 10 participants from the HMOG dataset for this study.

3.2 Data Pre-processing

Initially, the untreated sensor data streams underwent preliminary adjustments to purify signals and standardize distributions. In particular, filtering methods were applied to eliminate noise from the readings. Subsequently, the refined signals from accelerometers and gyroscopes were standardized to reduce variations across different sensor scales. Ultimately, the processed multi-sensor chronological sequences were partitioned into non-overlapping segments lasting 2.56 s each, employing a sliding window approach. This resulted in fixed-width instances, capturing user behavior patterns over time for the learning algorithms to analyze.

3.3 Training Deep Learning Models

We present SE-DeepConvNet, a concise CNN designed for continuous authentication based on sensor data. The model autonomously derives spatial representations through convolutional layers directly from the unprocessed input sequences. SE blocks are subsequently introduced to recalibrate feature responses channel-wise, amplifying informative features. Further optimization during training is achieved through additional batch normalization and ReLU activation layers, which normalize activations and address the vanishing gradient issue. Illustrated in Fig. 2, this cohesive structure facilitates effective learning of distinctive behavioral characteristics from sensor data noise, ensuring dependable user authentication.

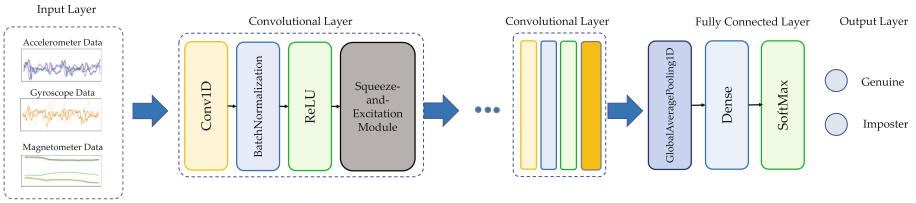

Fig. 2. The proposed SE-DeepConvNet model.

The recalibration of filter responses to accentuate significant features is achieved through SE blocks, initially introduced in [34]. These blocks function in two primary stages — squeeze and excitation. During the squeeze phase, spatial information is consolidated across channels through global average pooling to create channel-wise statistics. The subsequent excitation phase captures inter-channel dependencies using this aggregated information. More precisely, a straightforward gating mechanism employing two fully connected layers activated by ReLU and sigmoid functions, respectively, learns scalar weights for each channel. As demonstrated in Fig. 3, this re-weighting process selectively amplifies influential channels while suppressing less valuable ones, leading to enhanced representation learning.

3.4 Performance Measurement Criteria

The primary measures for evaluating authentication performance are three standard metrics. True Acceptance (TA) corresponds to accurately classifying patterns attributed to the legitimate user as Genuine. True Reject (TR) signifies the correct classification of patterns unrelated to the genuine user as an Imposter. Conversely, False Acceptance (FA) refers to misclassifying patterns not associated with the genuine user as Genuine. Finally, False Reject (FR) denotes the misclassification of patterns belonging to the genuine user as Imposter.

We assess the performance of authentication through three essential metrics:

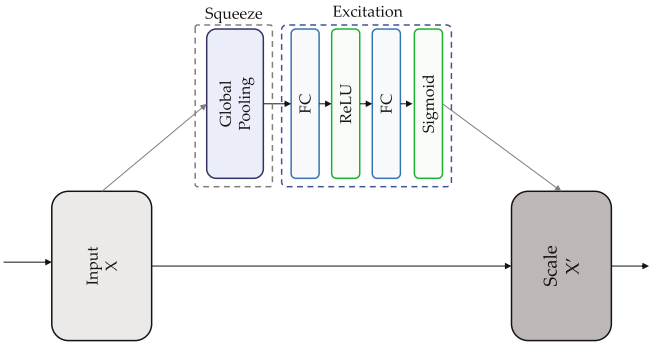

Fig. 3. The Squeeze-and-Excitation module.

1. False Acceptance Rate (FAR) quantifies the ratio of imposter access attempts wrongly identified as genuine users. Reduced values signify heightened security.
2. False Rejection Rate (FRR) measures the ratio of legitimate user attempts to erroneously denied access. Lower values prioritize user convenience.
3. Equal Error Rate (EER) denotes the error rate when FAR equals FRR. As FAR and FRR trade-off, EER balances security and convenience.

The mathematical formulas for these three metrics are presented as follows:

$$FAR = \frac{FA}{FA + TR} \tag{1}$$

$$FRR = \frac{FR}{FR + TA} \tag{2}$$

$$EER = \frac{FAR + FRR}{2} \tag{3}$$

where $|FAR + FRR|$ is minimum.

4 Experiments and Research Findings

In this section, we describe the experiments carried out to assess the proposed SE-DeepConvNet model for continuous authentication. We assess the model's performance on a publicly available dataset by employing data from accelerometer, gyroscope, and magnetometer sensors. We provide information on evaluation metrics, comparisons with baseline models, parameter configurations, and accuracy analyses across various sensing modalities. The presented vital findings showcase cutting-edge authentication rates, affirming the success of incorporating SE blocks into deep convolutional neural networks for reliable user verification from motion sequences captured by wearable devices.

4.1 Experimental Setting

The experimentation is conducted using Python on Google Colab Pro+ with the aid of a Tesla-V100 GPU to expedite computations. The assessments involve pitting the proposed SE-DeepConvNet model against conventional deep learning structures, such as standard CNNs and long short-term memory (LSTM) networks, specifically for continuous authentication based on sensor data. The comparative outcomes gauge enhancements in recognition achieved by incorporating SE blocks into our deep convolutional network.

4.2 Experimental Results and Discussion

The sensor dataset underwent partitioning through a 10-fold cross-validation protocol, ensuring a rigorous evaluation of the model's performance. The authentication results, showcased in Table 1, affirm the improvements introduced by the SE-DeepConvNet model. These results highlight its cutting-edge accuracy and EER compared to conventional methods.

Table 1. Performance metrics of baseline deep learning models including the proposed SE-DeepConvNet using HMOG dataset.

Gait-based Activity	CNN		LSTM		SE-DeepConvNet	
	EER(%)	Accuracy(%)	EER(%)	Accuracy(%)	EER(%)	Accuracy(%)
Read-Walk	0.75(±2.67)	99.51(±1.73)	0.60(±1.81)	99.60(±1.21)	0.38(±1.13)	99.78(±6.67)
Write-Walk	1.33(±2.86)	99.09(±1.86)	1.55(±2.79)	98.97(±1.82)	1.26(±2.32)	99.13(±1.55)
Map-Walk	1.24(±4.73)	99.08(±4.25)	0.77(±1.44)	99.48(±0.96)	0.83(±1.40)	99.43(±0.98)

Table 1 reveals noteworthy observations from the results, leading to several key findings. In the Read-Walk activity, where participants read while walking, the SE-DeepConvNet model demonstrates superior performance. It achieves the highest accuracy at 99.78% and the lowest EER at 0.379%, showcasing a substantial advancement over the baseline CNN and LSTM models.

In the Write-Walk activity involving writing while walking, the SE-DeepConvNet again outshines other models. It attains a top accuracy of 99.13% and an EER of 1.264%. However, the performance gap compared to baselines is slightly narrower than observed in Read-Walk. A similar trend is noticeable in the Map-Walk activity, where map navigation while walking is involved. Here, the SE-DeepConvNet exhibits a marginally higher accuracy of 99.431% and a lower EER of 0.829% compared to CNN and LSTM models.

The advantage gained from incorporating SE blocks is more pronounced in the Read-Walk activity than in other activities, suggesting that SE recalibration is particularly effective in this context. Notably, all models exhibit a comparatively lower performance in the Write-Walk activity than in other activities. This implies that writing while walking may introduce more variability or noise than reading or map-based interactions.

The findings from these experiments indicate that the SE-DeepConvNet surpasses alternative deep learning networks, achieving the highest accuracy at 99.778% and the lowest EER at 0.379% when applied to sensor data from the activity of reading while walking. In the case of the activity involving writing while walking, the SE-DeepConvNet outperforms the baseline deep learning models (CNN and LSTM). These comparative outcomes have been depicted graphically in Fig. 4.

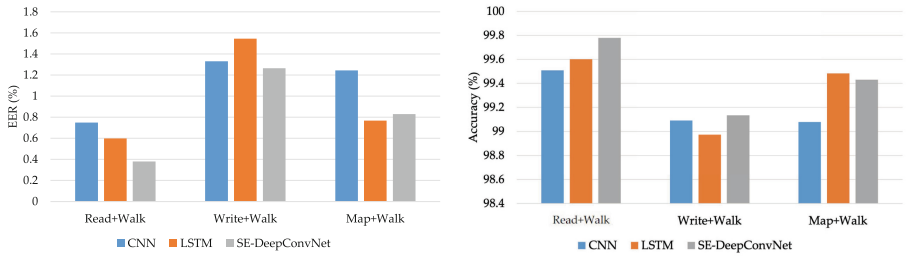

Fig. 4. Comparative results of deep learning models used in this work: (left side) EER, and (right side) accuracy.

5 Conclusion and Future Works

This research introduced SE-DeepConvNet, a CNN incorporating squeeze-and-excitation modules. These modules recalibrate feature responses channel-wise within each convolutional layer to highlight significant representations. The experiments conducted demonstrate cutting-edge authentication accuracy, reaching 99.78% and a low equal error rate of 0.38% on a publicly available gait analysis dataset, surpassing the capabilities of standard deep learning approaches.

Future endeavors in this line of research should focus on verifying our model's adaptability across diverse datasets encompassing various activity modalities. To boost performance, consideration could be given to implementing more sophisticated lightweight architectures and integrating data inputs transformed in time and frequency. In summary, the SE mechanism promises to ensure robust continuous verification using mobile sensor data.

Acknowledgments. This research project was supported by Thailand Science Research and Innovation Fund; University of Phayao under Grant No. FF67-UoE-214; National Science, Research and Innovation Fund (NSRF); and King Mongkut's University of Technology North Bangkok with Contract no. KMUTNB-FF-67-B-10.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Abo El-Soud, M.W., Gaber, T., AlFayez, F., Eltoukhy, M.M.: Implicit authentication method for smartphone users based on rank aggregation and random forest. Alex. Eng. J. **60**(1), 273–283 (2021). https://doi.org/10.1016/j.aej.2020.08.006
2. Baig, A.F., Eskeland, S., Yang, B.: Novel and efficient privacy-preserving continuous authentication. Cryptography **8**(1) (2024). https://doi.org/10.3390/cryptography8010003
3. Bimbot, F., et al.: A tutorial on text-independent speaker verification. EURASIP J. Adv. Signal Process. **2004**, 430-451 (2004). https://doi.org/10.1155/S1110865704310024
4. Buthpitiya, S., Zhang, Y., Dey, A.K., Griss, M.: n-gram geo-trace modeling. In: Lyons, K., Hightower, J., Huang, E.M. (eds.) Pervasive 2011. LNCS, vol. 6696, pp. 97–114. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-21726-5_7
5. Chen, L., Zhang, H., Xiao, J., Nie, L., Shao, J., Liu, W., Chua, T.: Sca-cnn: spatial and channel-wise attention in convolutional networks for image captioning. In: 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 6298–6306. IEEE Computer Society, Los Alamitos, CA, USA (2017). https://doi.org/10.1109/CVPR.2017.667
6. Choi, J., Choi, S., Kang, T.: Smartphone authentication system using personal gaits and a deep learning model. Sensors **23**(14) (2023). https://doi.org/10.3390/s23146395
7. Damaševičius, R., Vasiljevas, M., Salkevicius, J., Woźniak, M.: Human activity recognition in aal environments using random projections. Comput. Math. Methods Med. **2016**, 1–17 (2016). https://doi.org/10.1155/2016/4073584
8. Fathy, M.E., Patel, V.M., Chellappa, R.: Face-based active authentication on mobile devices. In: 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 1687–1691 (2015). https://doi.org/10.1109/ICASSP.2015.7178258
9. Gadaleta, M., Rossi, M.: Idnet: smartphone-based gait recognition with convolutional neural networks. Pattern Recogn. **74**, 25–37 (2018). https://doi.org/10.1016/j.patcog.2017.09.005
10. Giorgi, G., Saracino, A., Martinelli, F.: Using recurrent neural networks for continuous authentication through gait analysis. Pattern Recogn. Lett. **147**, 157–163 (2021). https://doi.org/10.1016/j.patrec.2021.03.010
11. Hinton, G.E., Osindero, S., Teh, Y.W.: A fast learning algorithm for deep belief nets. Neural Comput. **18**(7), 1527-1554 (2006). https://doi.org/10.1162/neco.2006.18.7.1527
12. Hu, J., Shen, L., Sun, G.: Squeeze-and-excitation networks. In: 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 7132–7141 (2018). https://doi.org/10.1109/CVPR.2018.00745
13. Ji, S., Xu, W., Yang, M., Yu, K.: 3d convolutional neural networks for human action recognition. IEEE Trans. Pattern Anal. Mach. Intell. **35**(1), 221–231 (2013). https://doi.org/10.1109/TPAMI.2012.59
14. Karpathy, A., Toderici, G., Shetty, S., Leung, T., Sukthankar, R., Fei-Fei, L.: Large-scale video classification with convolutional neural networks. In: 2014 IEEE Conference on Computer Vision and Pattern Recognition, pp. 1725–1732 (2014). https://doi.org/10.1109/CVPR.2014.223

15. Kašys, K., Dundulis, A., Vasiljevas, M., Maskeliūnas, R., Damaševičius, R.: BodyLock: human identity recogniser app from walking activity data. In: Gervasi, O., et al. (eds.) ICCSA 2020. LNCS, vol. 12250, pp. 307–319. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-58802-1_23
16. Li, Y., Hu, H., Zhou, G., Deng, S.: Sensor-based continuous authentication using cost-effective kernel ridge regression. IEEE Access **6**, 32554–32565 (2018). https://doi.org/10.1109/ACCESS.2018.2841347
17. Mantyjarvi, J., Lindholm, M., Vildjiounaite, E., Makela, S.M., Ailisto, H.: Identifying users of portable devices from gait pattern with accelerometers. In: Proceedings. (ICASSP2005). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005, vol. 2, pp. ii/973–ii/976 (2005). https://doi.org/10.1109/ICASSP.2005.1415569
18. Martinovic, I., Rasmussen, K., Roeschlin, M., Tsudik, G.: Authentication using pulse-response biometrics. Commun. ACM **60**(2), 108-115 (2017). https://doi.org/10.1145/3023359
19. Mekruksavanich, S., Jitpattanakul, A.: Deep residual network for smartwatch-based user identification through complex hand movements. Sensors **22**(8) (2022). https://doi.org/10.3390/s22083094
20. Mekruksavanich, S., Jitpattanakul, A.: Fallnext: a deep residual model based on multi-branch aggregation for sensor-based fall detection. ECTI Trans. Comput. Inform. Technol. (ECTI-CIT) **16**(4), 352-364 (2022). https://doi.org/10.37936/ecti-cit.2022164.248156
21. Muaaz, M., Mayrhofer, R.: An analysis of different approaches to gait recognition using cell phone based accelerometers. In: Proceedings of International Conference on Advances in Mobile Computing & Multimedia,MoMM 2013. pp. 293-300. Association for Computing Machinery, New York (2013). https://doi.org/10.1145/2536853.2536895
22. Muaaz, M., Mayrhofer, R.: Smartphone-based gait recognition: from authentication to imitation. IEEE Trans. Mob. Comput. **16**(11), 3209–3221 (2017). https://doi.org/10.1109/TMC.2017.2686855
23. Nickel, C., Busch, C., Rangarajan, S., Möbius, M.: Using hidden markov models for accelerometer-based biometric gait recognition. In: 2011 IEEE 7th International Colloquium on Signal Processing and its Applications, pp. 58–63 (2011). https://doi.org/10.1109/CSPA.2011.5759842
24. Nickel, C., Wirtl, T., Busch, C.: Authentication of smartphone users based on the way they walk using k-nn algorithm. In: 2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 16–20 (2012). https://doi.org/10.1109/IIH-MSP.2012.11
25. Papavasileiou, I., Qiao, Z., Zhang, C., Zhang, W., Bi, J., Han, S.: Gaitcode: gait-based continuous authentication using multimodal learning and wearable sensors. Smart Health **19**, 100162 (2021). https://doi.org/10.1016/j.smhl.2020.100162
26. Peinado-Contreras, A., Munoz-Organero, M.: Gait-based identification using deep recurrent neural networks and acceleration patterns. Sensors **20**(23) (2020). https://doi.org/10.3390/s20236900
27. Qi, M., Lu, Y., Li, J., Li, X., Kong, J.: User-specific iris authentication based on feature selection. In: 2008 International Conference on Computer Science and Software Engineering, vol. 1, pp. 1040–1043 (2008). https://doi.org/10.1109/CSSE.2008.1060
28. Shabrina, N., Isshiki, T., Kunieda, H.: Fingerprint authentication on touch sensor using phase-only correlation method. In: 2016 7th International Conference of

Information and Communication Technology for Embedded Systems (IC-ICTES), pp. 85–89 (2016). https://doi.org/10.1109/ICTEmSys.2016.7467127
29. Shiraga, K., Makihara, Y., Muramatsu, D., Echigo, T., Yagi, Y.: Geinet: view-invariant gait recognition using a convolutional neural network. In: 2016 International Conference on Biometrics (ICB), pp. 1–8 (2016). https://doi.org/10.1109/ICB.2016.7550060
30. Sitová, Z., et al.: Hmog: new behavioral biometric features for continuous authentication of smartphone users. IEEE Trans. Inf. Forensics Secur. **11**(5), 877–892 (2016). https://doi.org/10.1109/TIFS.2015.2506542
31. Taigman, Y., Yang, M., Ranzato, M., Wolf, L.: Deepface: closing the gap to human-level performance in face verification. In: 2014 IEEE Conference on Computer Vision and Pattern Recognition, pp. 1701–1708 (2014). https://doi.org/10.1109/CVPR.2014.220
32. Thang, H.M., Viet, V.Q., Dinh Thuc, N., Choi, D.: Gait identification using accelerometer on mobile phone. In: 2012 International Conference on Control, Automation and Information Sciences (ICCAIS), pp. 344–348 (2012). https://doi.org/10.1109/ICCAIS.2012.6466615
33. Wu, Y., He, K.: Group normalization. Int. J. Comput. Vision **128**, 742–755 (2018)
34. Xu, W., Shen, Y., Luo, C., Li, J., Li, W., Zomaya, A.Y.: Gait-watch: a gait-based context-aware authentication system for smart watch via sparse coding. Ad Hoc Netw. **107**, 102218 (2020). https://doi.org/10.1016/j.adhoc.2020.102218
35. Yang, J., Ren, Z., Gan, C., Zhu, H., Parikh, D.: Cross-channel communication networks. In: Wallach, H., Larochelle, H., Beygelzimer, A., d'Alché-Buc, F., Fox, E., Garnett, R. (eds.) Advances in Neural Information Processing Systems, vol. 32, pp. 1–10. Curran Associates, Inc. (2019)
36. 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 (2015). https://doi.org/10.1109/BTAS.2015.7358784
37. Zou, B., Li, Y.: Touch-based smartphone authentication using import vector domain description. In: 2018 IEEE 29th International Conference on Application-specific Systems, Architectures and Processors (ASAP), pp. 1–4 (2018). https://doi.org/10.1109/ASAP.2018.8445125