A One-Class Classification Method for Human Gait Authentication Using Micro-Doppler Signatures

Ji, Haoran ; Hou, Chunping ; Yang, Yang ; Fioranelli, Francesco; Lang, Yue

DOI
10.1109/LSP.2021.3122344

Publication date
2021

Document Version
Final published version

Published in
IEEE Signal Processing Letters

A One-Class Classification Method for Human Gait Authentication Using Micro-Doppler Signatures

Haoran Ji, Chunping Hou, Yang Yang, Francesco Fioranelli, *Senior Member, IEEE*, and Yue Lang

***Abstract*—In this letter, a radar-based gait authentication method is proposed. We focus on the overfitting problem on the target category caused by limited training data in authentication models and propose a one-class classification model to alleviate this problem. The effectiveness of such model is verified by establishing a radar-based gait dataset, which is composed of gait micro-Doppler spectrograms derived from nine human subjects. The experimental results demonstrate that, under the condition of limited training data, the performances of an authentication model degrade because misclassification of the non-target samples easily occurs. The proposed method effectively avoids this risk, performing the other existing authentication and one-class classification methods on the metric Equal Error Rate.**

***Index Terms*—Gait authentication, micro-Doppler radar, one class classification.**

I. Introduction

PERSON authentication has been a hot topic in the Internet of Things area. Many authentication systems employ different human traits, such as fingerprint [1] and iris [2], as the unique clue to recognize the identity of a person. Gait is one of the traits which is easy to collect and hard to camouflage, therefore, many gait-based person authentication algorithms have been proposed in decades [3]–[5].

Thanks to the capability of collecting human gaits in the dark environment and its good privacy-preserving nature compared to optical cameras, the radar is increasingly adopted in gait authentication problems in recent years. Thanks to the micro-Doppler effect, radar echoes contain rich gait information. Ni $et\ al.$ fine-tuned a pre-trained ResNet-50 with transfer learning to identify human subjects [6]. In [7], AlexNet was used to classify the 24 subjects' micro-Doppler signature. In general, most of the methods in literature use a multi-class classifier as an authenticator. However, in authentication problems, there are data only available for one target, hence the multi-class classifier is not a suitable solution.

Compared with the multi-class classification, one-class classification (OCC) is more suitable for the authentication problem. OCC algorithms only need the samples from one class (known as the target class) for training. During testing, well-trained one-class classifiers can recognize whether the input sample belongs to the target class or not. The authors of [8] extracted a set of human gait features and employed the OCC methods from the dd_tools toolbox [9] for person authentication. At the same time, since this work [8] employs handcrafted features for authentication problems, the performance of the proposed model may be degraded because of the poor generalization ability of handcrafted features.

The generative adversarial network (GAN) provides a feasible solution to the authentication problem. In the GAN-based OCC model, the discriminator is used as a one-class classifier, and the generator produces adversarial samples as the auxiliary support to train the discriminator. This is shown in Fig 1(b). However, such methods heavily rely on the diversity of the training set. In the radar-based authentication problem, the number of target data is usually limited. In this case, such methods are easily suffered the overfitting problem during training, and the classification boundary tends to be overly precise so that other unseen target samples are easily misclassified (see Fig. 1(c)).

To solve this problem, we propose a novel radar-based authentication method based on the vicinal risk minimization (VRM) principle [10], and it is named as augmentation generative adversarial network (AugGAN). The main idea of the VRM principle is to train the model by the extra samples from the vicinal domain, which is a vicinity or a neighborhood around each training sample. The authors of [11] point out that samples from the vicinal domain share the same class with the original data, and related experiments indicate that these vicinal samples can effectively support the training set. Overall, the key contributions can be summarized as follows:

- A novel authentication model has been proposed, which only utilizes the samples of the target's gait for training.
- The VRM principle is introduced into the OCC method and is implemented by adding an autoencoder into a standard GAN-based OCC scheme is proposed.
- The experimental results outperform better than both OCC methods and authentication methods. The superior performance verifies that using the VRM principle can solve the overfitting problem.

Manuscript received September 1, 2021; revised October 17, 2021; accepted October 20, 2021. Date of publication October 26, 2021; date of current version November 23, 2021. This work was supported by the National Natural Science Foundation of China under Grants 62101378 and 62171318. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Jun Liu. *(Corresponding author: Yang Yang.)*

Haoran Ji is with Tianjin International Engineering Institute, Tianjin University, Tianjin 300072, China (e-mail: jhr0618@tju.edu.cn).

Chunping Hou and Yang Yang are with the School of Electrical and Information Engineering, Tianjin University, Tianjin 300072, China (e-mail: hcp@tju.edu.cn; yang_yang@tju.edu.cn).

Francesco Fioranelli is with the MS3 Section, Department of Microelectronics, TU Delft, 2628CD Delft, The Netherlands (e-mail: f.fioranelli@tudelft.nl).

Yue Lang is with the School of Electronic and Information Engineering, Hebei University of Technology, Tianjin 300401, China (e-mail: langyue@hebut.edu.cn).

Digital Object Identifier 10.1109/LSP.2021.3122344

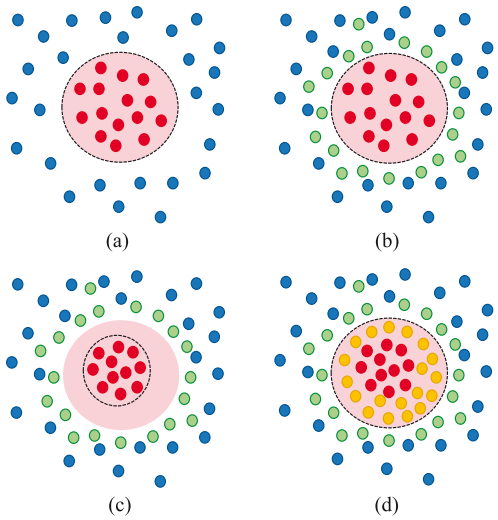

Fig. 1. Sketches of the OCC concept. The red circle represents the target sample, the blue circle represents the non-target sample, the pink area represents the target sample space, the black dashed line represents the classification boundary, the green circle represents the adversarial sample, and the yellow circle represents the enhanced sample. (a) the ideal one-class classifier. (b) The ideal GAN-based one-class classifier. (c) The real GAN-based one-class classifier. (d) The proposed classifier in this work.

II. Data Acquisition and Pre-Processing

The movement of individual body parts reflects into the micro-Doppler signature, which is the data format typically used for radar-based traits of human gaits [12], [13].

We acquire the human gait data in an indoor environment using the ultra-wideband (UWB) impulse mono-static radar named PulsON 440 (P440) with two horn antennas. The P440 operates at the center frequency of 4.3 GHz with a pulse repetition frequency (PRF) of 368 Hz.

The dataset contains 6 males and 3 females of age between 22 and 28 years. For 10 times each participant walked freely within 1 to 6 m from the radar, hence generating 90 radar recordings in total.

Each radar echo is a time-range profile of about 6 seconds; these are processed to extract the micro doppler signature [14]. First, we implement the data augmentation [15] by using a sliding window over time to crop the time-range profiles into several segments. Consequently the length of each segment is determined only by the length of the sliding window [16]. A 1.2 s duration of the sliding window is chosen to ensure that the semantic of common human motion can be adequately recorded. Then, we use the average background subtraction on each segment to remove the static background information. Finally, we adopt time-frequency analysis, short-time Fourier transform (STFT) in this letter, to visualize the micro-Doppler signature.

III. Proposed Method for Gait-Based Authentication

In this section, we elaborated a two-branch GAN named the AugGAN, which is a method based on the VRM principle and composed with the high-quality autoencoder (HQAE), the low-quality autoencoder (LQAE) and a discriminator. The block diagram of the method is shown in Fig 2.

A. Vicinal Risk Minimization

Most of the deep learning training process is based on the empirical risk minimization (ERM) principle [17]. The goal of training is to minimize the empirical risk based on the training set $D = (x_i, y_i)_{i=1}^n$, where x_i indicates the data and y_i indicates the label. The empirical risk can be written as:

$$R_e(f) = \frac{1}{n}\sum_{i=1}^{n} l(f(x_i), y_i), \tag{1}$$

where l indicates the loss function.

Researchers often transform the OCC problem into the binary classification problem. They adopt GANs to automatically generate adversarial samples as the non-target datasets $D_{adv} = (\hat{x_i}, 0)_{i=1}^n$. The discriminator is trained by both $D = (x_i, 1)_{i=1}^n$ and $D_{adv} = (\hat{x_i}, 0)$ at the same time. The discriminator's empirical risk can be written as:

$$R_e(f) = \frac{1}{n}\sum_{i=1}^{n} l(f(x_i), 1) + l(f(\hat{x_i}), 0) \tag{2}$$

In the case of limited training samples, this empirical risk results in the overfitting [17]. To alleviate this problem, the VRM principle has been proposed. Unlike ERM, VRM uses an extra prior to solve this problem. Specifically, it uses a vicinal distribution P_v to construct a dataset $D_v = (\tilde{x_i}, \tilde{y_i})_{i=1}^n$ and minimize the empirical vicinal risk $R_v(f)$:

$$P_v(x, y) = \frac{1}{n}\sum_{i=1}^{n} v\left(\tilde{x}, \tilde{y} | x_i, y_i\right) \tag{3}$$

$$R_v(f) = \frac{1}{n}\sum_{i=1}^{n} l\left(f(\tilde{x_i}), \tilde{y_i}\right) \tag{4}$$

We propose the learnable vicinal distribution $P_{\tilde{v}}(\tilde{x}, 1)$ by adding an autoencoder into a standard GAN, which is the main contribution of this letter. The goal of the AugGAN is to minimize the empirical vicinal risk $R_{AugGAN}(f)$:

$$R_{AugGAN}(f) = \frac{1}{n}\sum_{i=1}^{n}[l(f(x_i), 1) + l(f(\tilde{x_i}), 1) + l(f(\hat{x_i}), 0)] \tag{5}$$

The target dataset $D = (x_i, 1)_{i=1}^n$, the augmented dataset $D_v = (\tilde{x_i}, 1)_{i=1}^n$ and the adversarial dataset $D_{adv} = (\hat{x_i}, 0)_{i=1}^n$ are all used to train the discriminator.

B. Discriminator

The discriminator consists of three convolutional layers and a fully connected layer. Sigmoid is used as the activation function and maps the outputs of the classifier to the probability that the input sample belongs to the target class. The input of the discriminator has three parts: target samples, augmented samples output of the HQAE, and adversarial samples output of the

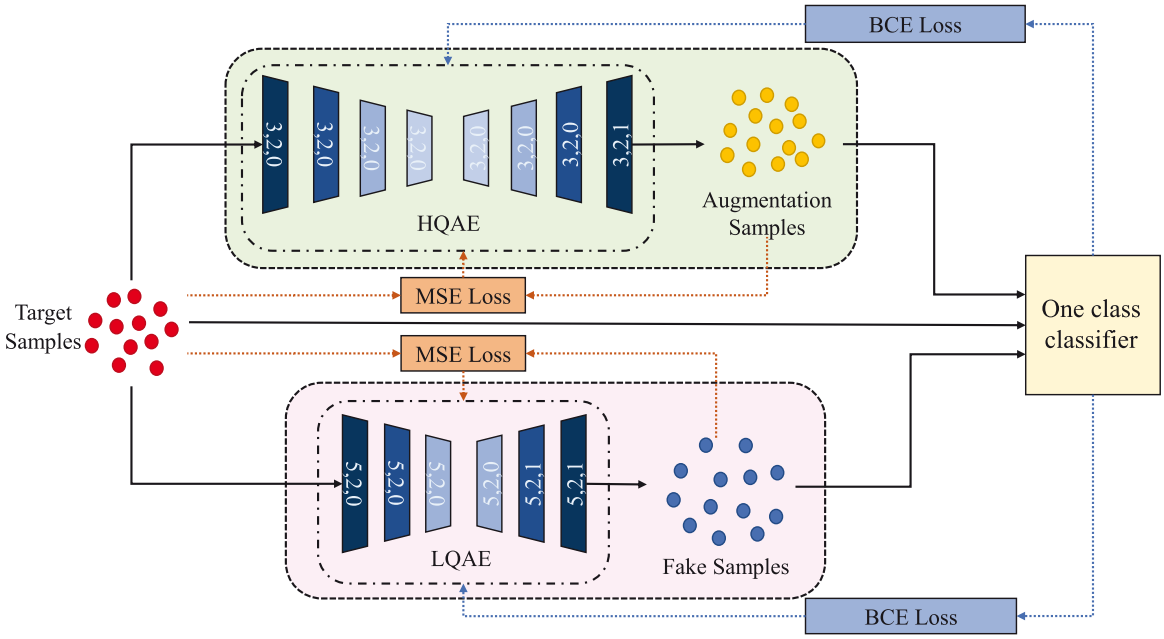

Fig. 2. The network architecture of the AugGAN. The values [x, y, z] depicted in each convolutional layer correspond to the kernel, stride and padding.

LQAE. According to the VRM principle, the AugGAN treats augmented samples as targets. We use the binary cross-entropy (BCE) loss to train the discriminator:

$$\begin{aligned} L_{cls} = & -E_{x\sim\mathcal{P}_r}[logD(x)] \\ & -E_{x\sim\mathcal{P}_r}[log(D(HQAE(x)))] \\ & -E_{x\sim\mathcal{P}_r}[log(1-D(LQAE(x))], \end{aligned} \tag{6}$$

where D indicates the discriminator network.

C. Two Autoencoders

The two autoencoders help train the discriminator by generating auxiliary samples. A two-branch GAN model is a GAN with 2 modules for data generation. The HQAE has three convolutional layers and three deconvolutional layers. The LQAE has five convolutional layers and five deconvolutional layers. The kernel size in the HQAE is 5×5 and in the LQAE is 3×3. The strides of both of them are 2. Both autoencoders first map the input into a latent space as a vector, then the corresponding vector are separately reconstructed into a sample as similar as possible to the original input. The mean square error (MSE) loss is used in both the HQAE and the LQAE, the MSE loss is shown as:

$$\begin{aligned} L_{MSE} = E_{x\sim\mathcal{P}_r}\left[||x-HQAE(x)||_2^2\right. \\ \left.+||x-LQAE(x)||_2^2\right], \end{aligned} \tag{7}$$

where $\mathcal{P}_r$ refers to the distribution of the target samples, and $AE(x)$ is the output of the HQAE or the LQAE. Furthermore, the binary cross entropy (BCE) loss is also adopted in training process:

$$\begin{aligned} L_{BCE} = & -E_{x\sim\mathcal{P}_r}[log(D(HQAE(x))) \\ & +log(D(LQAE(x)))] \end{aligned} \tag{8}$$

Compared with the one-branch GAN, e.g. the ALOCC [22], the two-branch GAN has two networks for data generation. By utilizing the HQAE and the LQAE, the AugGAN generates two kinds of samples, including augmented samples $\tilde{x_i}$ to overcome the over-fitting problem and adversarial samples $\hat{x_i}$ for adversarial training.

The autoencoders are optimized based on the outputs of the discriminator. It is worth noting that although we employ the BCE loss for both autoencoders, their training goals are different. During the training process of the discriminator, the outputs of the HQAE and the LQAE are seen as different categories. Thus, the HQAE is trained to make its outputs as similar as the target samples and the LQAE is trained so that its outputs can be seen as the non-target samples.

D. Training Process

During each iteration, the proposed AugGAN is trained following two steps. In the first step, the HQAE and LQAE are trained firstly. At the same time, the parameters on the discriminator are frozen. Next, the HQAE and LQAE are fixed, and the discriminator is trained. In this step, the auxiliary samples are generated by both autoencoders at first, then the training is driven by both auxiliary and original training samples. Algorithm 1 summarizes the training process.

IV. Experiment and Results

A. Experimental Setup and Implementation Details

As mentioned in Section II, each subject is recorded by radar 10 times. Then, these sequences of each subject are randomly grouped into 5 parts. In each part, there are 2 sequences of radar raw data. According to the signal processing and data augmentation mentioned in Section II, we obtain 400 spectrograms

TABLE I
THE EER PERFORMANCES OF THE AUGGAN AND OTHER COMPARISON ALGORITHMS

	Target 1	Target 2	Target 3	Target 4	Target 5	Target 6	Target 7	Target 8	Target 9	Mean
HF+Gauss [8]	0.351	0.514	0.461	0.590	0.509	0.488	0.249	0.621	0.506	0.477
AnoGAN [18]	0.567	0.351	0.566	0.506	0.449	0.440	0.454	0.380	0.327	0.449
f-AnoGAN [19]	0.481	0.363	0.504	0.510	0.467	0.527	0.468	0.462	0.395	0.464
GANomaly [20]	0.226	0.414	0.376	0.403	0.343	0.441	0.261	0.444	0.371	0.364
OC-ACNN [21]	0.445	0.471	0.454	0.459	0.463	0.453	0.444	0.463	0.465	0.457
ALOCC [22]	0.366	0.409	0.375	0.356	0.375	0.342	0.369	0.390	0.378	0.374
OCGAN [23]	0.214	0.394	0.290	0.432	0.397	0.320	0.280	0.339	0.384	0.339
OpenGAN [24]	0.245	0.323	0.321	0.511	0.405	0.314	0.269	0.448	0.370	0.356
AugGAN	**0.089**	**0.246**	**0.154**	**0.284**	**0.296**	**0.236**	**0.106**	**0.287**	**0.304**	**0.222**

Algorithm 1: Training process of the AugGAN.

Require: Set of training data x, iteration size N
Ensure: Models: HQAE, LQAE, D
1: **for** iteration 1 to $\rightarrow N$ **do** $\mathcal{N}(0,1)$
2: HQAE and LQAE update: keep D fixed.
3: $l_{MSE} \leftarrow ||x - HQAE(x)||_2^2 + ||x - LQAE(x)||_2^2$
4: $l_{BCE} \leftarrow D(HQAE(x),1) + D(LQAE(x),1)$
5: Back-propagate $l_{MSE} + l_{BCE}$ to update HQAE and LQAE
6: D update: keep HQAE, LQAE fixed
7: $l_D \leftarrow D(x,1) + D(HQAE(x),1) + D(LQAE(x),0)$
8: Back-propagate l_D to update D
9: **end for**

for each part. In one experiment, four hundred spectrograms in one part are selected as the training set, and the testing set is composed of both the other spectrograms of the same subject (400 spectrograms/parts $\times$ 4 parts) and the spectrograms of other subjects (400 spectrograms/(part $\times$ subject) $\times$ 5 parts $\times$ 8 subjects). We conduct 45 experiments for all parts, and finally, get 45 authenticators for 9 subjects in total. In order to evaluate the performance of these authenticators, the Equal Error Rate (EER), which is the most commonly used metric in authentication problems, is adopted in this letter. We listed the mean EER of 5 authenticators for each subject in Table I.

All experiments were implemented with PyTorch and worked on the workstation with the NVIDIA GeForce GTX 1080Ti Graphics Processing Unit (GPU) and an Intel Core I7-7700 k processor. The adaptive moment estimation (Adam) optimizer was used to optimize the models with a fixed learning rate of 2×10^{-4}. The network was trained for 100 epochs in each experiment, with a mini-batch size of 32. Five-fold cross-validation was carried out in the experiments to obtain stable results.

B. Experimental Results

We analyzed the AugGAN's performance by comparing it with other one-class algorithms [18]–[20], [23], [24] and two authentication algorithms [8], [21]. From Table I, the AugGAN outperforms other comparison algorithms and achieves an average EER of 0.222. This result proves that using the VRM principle in the OCC algorithm can alleviate the overfitting caused by the limited target samples. Among these algorithms, the performance of Ref. [8] is the worst, which proves that handcrafted features suffer from generalization problems.

In terms of the usage of the adversarial samples, the other OCC algorithms can be divided into two types: the metric-learning-based algorithms and the generative-model-based algorithms. The former contains the AnoGAN, f-AnoGAN and GANomaly, which regard the adversarial samples as the target samples and adopt the reconstruction error to form a metric space for classification. By assuming the error as the anomaly score, the classification result is determined under some metric criterion such as L2 distance. However, this assumption easily expands the distribution of the target category, hence non-target samples are prone to misclassification. The OC-ACNN, ALOCC, OCGAN, and OpenGAN can be categorized as generative-model-based algorithms. The authors of these approaches hold the view that the generated adversarial samples can be used to train the discriminator by treating them as non-target training samples. So, these continually generated negative samples can effectively improve the robustness of the model by alternative training. However, the number of iterations needs to be set carefully, because when the quantity of training dataset is limited, the classification boundary is increasingly compacted, which can seriously deteriorate the performance of these models. Overall, the AugGAN generates both the augmented samples and the adversarial samples, ensures the classification boundary is not compact or loose, achieves the best performance among these algorithms.

V. CONCLUSION

In this letter, a novel person authentication method using the micro-Doppler signature was proposed. Since the gait data is not enough for proper training of the classifier, we adopted the VRM principle to train the model and used the two-branch GAN to generate the augmented data and the adversarial data, respectively. A UWB radar was used to measure micro-Doppler signatures of nine people, constructing a dataset to verify the proposed AugGAN method. The experimental results showed that the AugGAN outperformed other OCC classifiers as well as existing authentication methods, achieving an average EER of 0.222 on the nine-person gait dataset.

REFERENCES

[1] K. K. Shreyas, S. Rajeev, K. Panetta, and S. S. Agaian, "Fingerprint authentication using geometric features," in *Proc. IEEE Int. Symp. Technol. Homeland Secur.*, 2017, pp. 1–7.

[2] B. John, S. Koppal, and E. Jain, "EyeVEIL: Degrading iris authentication in eye tracking headsets," in *Proc. 11th ACM Symp. Eye Tracking Res. Appl.*, 2019, pp. 1–5.

[3] T. H. Lam and R. S. Lee, "Human identification by using the motion and static characteristic of gait," in *Proc. 18th Int. Conf. Pattern Recognit.*, vol. 3, 2006, pp. 996–999.

[4] F. Sun, C. Mao, X. Fan, and Y. Li, "Accelerometer-based speed-adaptive gait authentication method for wearable IoT devices," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 820–830, Feb. 2019.

[5] T. Zhu, L. Fu, Q. Liu, Z. Lin, Y. Chen, and T. Chen, "One cycle attack: Fool sensor-based personal gait authentication with clustering," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 553–568, 2021, doi: 10.1109/TIFS.2020.3016819.

[6] Z. Ni and B. Huang, "Human identification based on natural gait micro-Doppler signatures using deep transfer learning," *IET Radar, Sonar Navi.*, vol. 14, no. 10, pp. 1640–1646, 2020.

[7] P. Cao, W. Xia, M. Ye, J. Zhang, and J. Zhou, "Radar-ID: Human identification based on radar micro-Doppler signatures using deep convolutional neural networks," *IET Radar, Sonar Navi.*, vol. 12, no. 7, pp. 729–734, 2018.

[8] A. Arra *et al.*, "Personalized gait-based authentication using UWB wearable devices," in *Proc. 27th ACM Conf. User Model., Adapt. Personalization*, 2019, pp. 206–210.

[9] D. Tax, "Data description toolbox dd tools 2.0.0," Delft Univ. Technol., Delft, The Netherlands, 2013. [Online]. Available: http://homepage.tudelft.nl/n9d04/dd_manual.pdf

[10] O. Chapelle, J. Weston, L. Bottou, and V. Vapnik, "Vicinal risk minimization," in *Proc. Adv. Neural Inf. Process. Syst.*, 2001, pp. 416–422.

[11] H. Zhang, M. Cisse, Y. N. Dauphin, and D. Lopez-Paz, "Mixup: Beyond empirical risk minimization," in *Proc. Int. Conf. Learn. Representations*, 2011, *arXiv:1710.09412*.

[12] V. C. Chen, F. Li, S.-S. Ho, and H. Wechsler, "Analysis of micro-Doppler signatures," *IEE Proc.-Radar, Sonar Navi.*, vol. 150, no. 4, pp. 271–276, 2003.

[13] D. Tahmoush and J. Silvious, "Radar micro-Doppler for long range front-view gait recognition," in *Proc. IEEE 3rd Int. Conf. Biom.: Theory, Appl., Syst.*, 2009, pp. 1–6.

[14] B. Erol, S. Z. Gurbuz, and M. G. Amin, "Motion classification using kinematically sifted ACGAN-synthesized radar micro-Doppler signatures," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 4, pp. 3197–3213, Aug. 2020.

[15] J. Park, R. J. Javier, T. Moon, and Y. Kim, "Micro-Doppler based classification of human aquatic activities via transfer learning of convolutional neural networks," *Sensors*, vol. 16, no. 12, p. 1990, 2016.

[16] R. J. Javier and Y. Kim, "Application of linear predictive coding for human activity classification based on micro-Doppler signatures," *IEEE Geosci. Remote Sens. Lett.*, vol. 11, no. 10, pp. 1831–1834, Oct. 2014.

[17] V. N. Vapnik, "An overview of statistical learning theory," *IEEE Trans. Neural Netw.*, vol. 10, no. 5, pp. 988–999, Sep. 1999.

[18] T. Schlegl, P. Seeböck, S. M. Waldstein, U. Schmidt-Erfurth, and G. Langs, "Unsupervised anomaly detection with generative adversarial networks to guide marker discovery," in *Proc. Int. Conf. Inf. Process. Med. Imag.*, Boone, NC, USA, 2017, pp. 146–157.

[19] T. Schlegl, P. Seeböck, S. M. Waldstein, G. Langs, and U. Schmidt-Erfurth, "f-AnoGAN: Fast unsupervised anomaly detection with generative adversarial networks," *Med. Image Anal.*, vol. 54, pp. 30–44, 2019.

[20] S. Akcay, A. Atapour-Abarghouei, and T. P. Breckon, "GANomaly: Semi-supervised anomaly detection via adversarial training," in *Proc. Asian Conf. Comput. Vision*, Perth, Australia, 2018, pp. 622–637.

[21] P. Oza and V. M. Patel, "Active authentication using an autoencoder regularized CNN-based one-class classifier," in *Proc. 14th IEEE Int. Conf. Autom. Face Gesture Recognit.*, 2019, pp. 1–8.

[22] M. Sabokrou, M. Khalooei, M. Fathy, and E. Adeli, "Adversarially learned one-class classifier for novelty detection," in *Proc. IEEE Conf. Comput. Vision Pattern Recognit.*, Salt Lake City, UT, USA, 2018, pp. 3379–3388.

[23] P. Perera, R. Nallapati, and B. Xiang, "OCGAN: One-class novelty detection using GANs with constrained latent representations," in *Proc. IEEE Conf. Comput. Vision Pattern Recognit.*, Long Beach, CA, USA, 2019, pp. 2898–2906.

[24] Y. Yang, C. Hou, Y. Lang, D. Guan, D. Huang, and J. Xu, "Open-set human activity recognition based on micro-Doppler signatures," *Pattern Recognit.*, vol. 85, pp. 60–69, 2018.