

# Code Division Modulation Layers Against Forgetting and Inference in Continual Gait Identification

Simone Milani

Department of Information Engineering, University of Padova, Padova, Italy  
simone.milani@dei.unipd.it

**Abstract**—Continual learning (CL) has been recently employed in biometric identification systems thanks to its ability to integrate new knowledge within a pre-trained model and to the possibility of reducing the computational cost of training. Unfortunately, such approaches pose new challenges both in terms of final accuracy and privacy guarantees since a progressive fine-tuning of the model on small subsets expose them to catastrophic forgetting and successful inference attacks.

This paper evaluates the efficiency of code division modulation layers (CDML) on a gait identification system which has been trained following a continual learning policy. The proposed approach preserves accuracy on all the tasks while mitigating membership inference attacks at the same time. Moreover, the impact of retransmission is minimized since replaying data is not necessary.

**Index Terms**—continual learning, membership inference, catastrophic forgetting, modulation, gait identification

## I. INTRODUCTION AND RELATED WORKS

Learning-based biometric systems have recently focused on studying continual learning (CL) approaches [1] in order to integrate new data, individuals or datasets into a pre-trained model (see the block diagram in Fig. 1). This interest arises from the computational limitations posed to retraining a model from scratch whenever an update is needed [2] and from privacy policies that may prevent biometric data sharing across different stages or terminals [3]. Moreover, behavioral biometrics are often characterized by non-stationary and time-varying templates depending on the acquisition contexts and conditions of the subjects [4]. Indeed, updating the model step-by-step (or task-by-task) permits protecting sensitive information during updates and constraining the computational load, and often, these solutions are implemented in a federated [5] or differential privacy set-up [6].

Unfortunately, CL solutions enable flexibility but pose new problems and challenges. One of the major ones is *catastrophic forgetting*, i.e., the information related to the first learning stages is lost after a few stages of training, and hence, the accuracy of the model reduces on the first classes or modalities. In order to mitigate this, several solutions were proposed ranging from replaying previous data [7], using

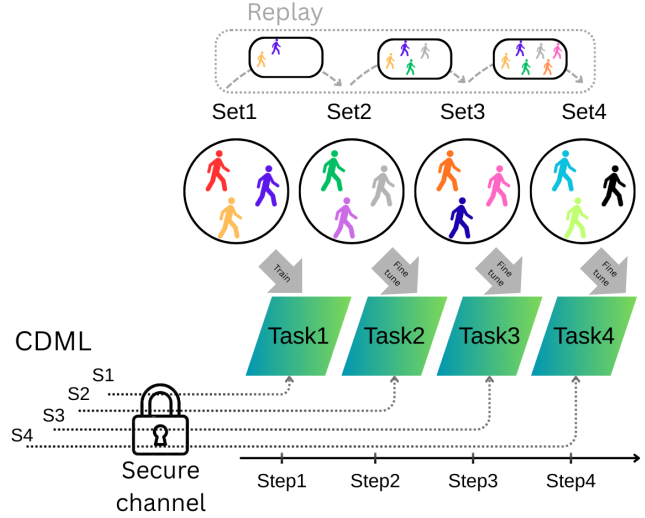


Fig. 1. Continual Learning scheme for gait-based identification. The block diagram reports the eventual replay strategy and the use of CDML information to mitigate catastrophic forgetting.

coarse-to-fine knowledge distillation [8], adopting modulation layers that remap the learned features [9], [10] or injecting data correlated with previous information and created with generative models [11], to mention some of them.

All these solutions mitigate the performance decrement, but produce a decrement in the privacy level since some sensitive information needs to be shared across tasks (see the diagram in Fig. 1).

Moreover, a second problem concerns the possibility of non-disclosing the partial datasets of each task by sharing the model only. Since the size of the trained network is dimensioned on the final overall task, the amount of data used to train the network at each task results limited. This exposes the generated network to possible Membership Inference Attacks (MIA) or Identity Inference Attacks (IIA). These attacks denote all those strategies that aims at inferring whether a given sample (MIA) or class/subject (IIA) was used in the training set of the probed model [12], [13]. Such strategies have been designed for classifiers [14], [15], generative models [16], and biometric recognition systems [17]. Indeed, success probabilities of attacks increase as the cardinality of training

We thank the partnership and collaboration with the São Paulo Research Foundation (Fapesp) Horus project, Grant #2023/12865-8. This manuscript reflects only the authors' views and opinions, neither EU nor the European Commission nor FAPESP can be considered responsible for them. All of the authors have revised the document and confirm the findings.

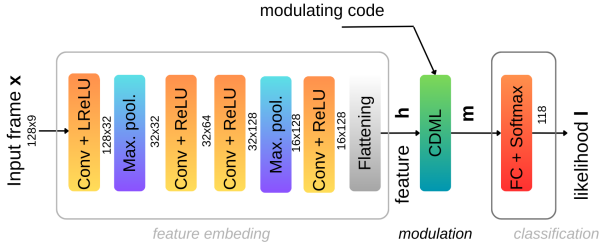


Fig. 2. Network structure from [18] with the additional CDML layer.

datasets reduces with respect to the size of the model [14], [16].

The current paper proposes a class-incremental continual learning strategy for gait identification that aims at solving both catastrophic forgetting and exposure to inference attacks by including a Code Division Modulating Layer (CDML) on the feature space that embeds the input signal to be classified. The approach is applied to the gait classifier reported in [18] and deployed in a continual learning set-up where users are divided across multiple tasks. Experimental results show that the final accuracy in classification is maximized while preventing inference in a black box scenario.

The main novelties introduced by the paper can be summarized as follows.

- The paper analyzes the impact of different countermeasures against catastrophic forgetting in Continual Learning from the privacy perspective by measuring the success probability of membership inference attacks.
- A novel Code Division Modulating Layer (CDML) is introduced in order to mitigate both the accuracy loss and the possibility of membership inference on a standard gait identification classifier. The proposed solution does not necessarily require the transmission of replay data, thus minimizing the transmission and storage needs.
- The different methods are then combined together to identify the most effective solution.
- An experimental validation of both classification accuracy and privacy level is performed for each solution. Results show that the proposed scheme improves identification performance with negligible impact on robustness and complexity.
- The approach enables granting different privacy levels to different users according to which modulating codes are shared.

These aspects are detailed in the following subsections.

## II. THE PROPOSED APPROACH

The starting point of the proposed approach is the CNN-based gait identification model in [18], which was chosen since results can be easily generalized and its structure can be well adapted to low-power devices with minimal quality loss as shown in [19]. The general structure is reported in Fig. 2 (gray circled blocks), together with the additional CDML layer proposed by this work. The network is made by

TABLE I  
COMPARISON OF A UNIFORM AND GAUSSIAN DISTRIBUTION AND DIFFERENT GENERATORS USING STATISTICAL TESTS.

| Dist/Gen.     | CS        | PCC       | KS Test | Run Test |
|---------------|-----------|-----------|---------|----------|
| Uniform Dist  | -2.09e-07 | -2.13e-07 | 0.506   | -0.0195  |
| Gaussian Dist | 5.28e-03  | 1.43e-06  | 0.186   | 0.0115   |
| Hénon Map     | 1.27e-03  | 7.32e-05  | 0.365   | 0.485    |
| Logistic Map  | 7.97e-03  | 2.52e-05  | 0.198   | 4.326    |
| Tent Map      | 8.43e-03  | 1.30e-05  | 0.144   | 2.496    |
| LCG           | -1.46e-05 | -1.38e-05 | 0.505   | -0.005   |

1D Convolutional layers, followed by ReLU activations and MaxPooling layers. The input is an array of 128 samples with 9 dimensions corresponding to the Inertial Measurement Unit (IMU) of a cellphone (more details in [18]).

Whenever the training set is decomposed into multiple subsets associated with a CL task, catastrophic forgetting occurs and therefore, mitigation strategies may involve replaying previous data or using prototypes.

As for replay solutions, the current paper refers to the work [7] where a percentage of samples from Tasks  $1, \dots, k-1$  are used to train the network for Task  $k$ . Another possible countermeasure is the inclusion of a Feature-wise Linear Modulation (FiLM) layer [9] that adapts the features  $\mathbf{h} = f(\mathbf{x})$  from the embedding layer using a set of weights  $\gamma_k$  and biases  $\beta_k$ , where both  $\gamma_k$  and  $\beta_k$  are computed during the incremental training at step/task  $k$ . This approach was first introduced in the general field of Continual Learning in [9], and it has been recently used for adaptation in gait identification [20]. The solution allows avoiding replaying data and preserves previously-learned features thus keeping the detection accuracy high. Unfortunately, it requires the transmission of parameters  $\gamma_k, \beta_k$  to the next classifier. Indeed, diversified privacy levels are enabled since each terminal can be provided with customizable detection capabilities depending on which set of  $\gamma_k, \beta_k$  is used.

The proposed approach implements a code division modulation on features  $\mathbf{h}$  by generating a set of uncorrelated sequences  $\mathbf{s}_k$ ,  $k = 1, \dots, N$ , where  $s_{k,i} \in \{-1, +1\}$  and  $\mathbf{s}_k \cdot \mathbf{s}_h \approx 0 \forall k \neq h$ . Sequences are created using a pseudo-random generator followed by a quantization stage. The seed is transmitted to the final enabled users through a secure channel (not publicly-distributed), who can re-generate the full sequence. Once the sequence is generated, it stays fixed and is not altered during the training process.

The modulated features

$$\mathbf{m} = \mathbf{s}_k \odot \mathbf{h} \quad (1)$$

are then processed by the classification layer and mapped into a likelihood array  $\mathbf{l} = g(\mathbf{m})$ , which will provide the outcome of the classification.

This processing step is analogous to Code Division Multiple Access (CDMA) systems in communications and allows embedding data from different tasks into uncorrelated feature spaces. In this way, even if the input samples (associated to different IDs) are mapped into a common latent region (because of signal similarities), feature modulation separates

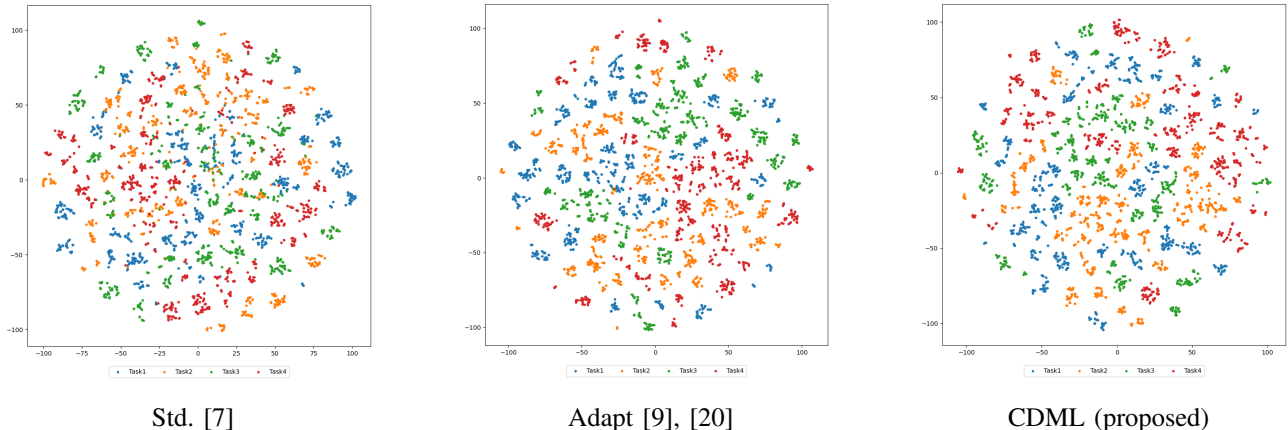


Fig. 3. Plots of t-SNE projections for the latent representation associated to different CL solutions. Different colors are associated to samples belonging to different tasks.

them into diverse uncorrelated areas thus enabling a correct classification.

This allows protecting training data from inference attacks as described in the following section.

From these premises, the crucial requirement for the selected random noise generator is the ability to create uncorrelated modulation sequences. For this purpose, two metrics have been used to measure correlation (*cosine similarity (CS)* and *Pearson correlation coefficient (PCC)*) between different sequences generated by the considered algorithms. Two other measures assess the randomness level of the generated sequence: the (*Kolmogorov-Smirnov test (KS test)* and the *Wald-Wolfowitz runs test (run test)*) [21]. The analysis has been performed over four different pseudorandom functions: *Hénon noise* [22], *Logistic map* [23], *Tent map* [24] and *Linear Congruential Generator (LCG)* [25]. Each function output has been normalised into the range  $[-1, 1]$  and results are reported in Table I.

In order to evaluate the impact of the modulation scheme on the final latent representation, t-SNE algorithm was applied on the feature arrays associated to test data. In this evaluation, testing considered a standard replay (Std.), learned-adaptation (Adapt), and the proposed strategy. Experimental results are reported in Fig. 3, and it is possible to notice that CDML achieves a better homogeneity in region organization.

### III. INFERENCE ATTACKS

In literature, different MIA strategies have been proposed during the last years. This work focuses on black box attacks where the inner structure of the network and weight values are not known by the attacker. Indeed, the attacker wants to verify whether a given couple  $(\mathbf{x}_i, \text{id}_i)$  belongs to the training set or not, where  $\mathbf{x}_i$  is the input sample and  $\text{id}_i$  is the corresponding ground truth label.

In this work, a confidence-based MIA attack (based on LiRA) was implemented [14], [15], where likelihoods  $1 = g(\mathbf{m})$  are computed and the value  $1[\text{id}_i]$  is compared to a

TABLE II  
SUBSET PARTITIONING ACROSS DIFFERENT TASKS

|          | Task 1 | Task 2  | Task 3  | Task 4   |
|----------|--------|---------|---------|----------|
|          | Set 1  | Set 2   | Set 3   | Set 4    |
| Subjects | 0 – 29 | 30 – 59 | 60 – 89 | 90 – 118 |

threshold. If the value is higher, it is possible to assume that the model displays a high confidence in the classification results and therefore, the sample is likely to belong to the training set.

Better strategies have been proposed in literature (e.g., using gradients, shadow models, etc.), but experimental results show that on the networks in [18] this strategy is sufficiently successful despite the limited size of the models.

### IV. EXPERIMENTAL SET-UP AND RESULTS

#### A. Setting

In the experiments, the training set is divided into 4 subsets including separate sets of subjects/users as reported in Table II. Subjects from dataset 1 of [18] are divided into groups of 30 persons and associated to 4 different tasks. Input data are made of 6 or 9 dimensional arrays of 128 samples, which were segmented from longer sequences according to gait cycles. Dataset acquisition and preparation are described in [18]. At first, the network is trained on set1, and then fine-tuned on the following subsets for 400 epochs with an exponentially decaying learning rate (starting at 0.001 with factor 0.9).

The proposed CDML strategy is compared with state-of-the-art replay strategies [7], where a percentage of previous datasets is transmitted to the following tasks. The percentage of re-processed data may be tuned according to the average accuracy.

In addition, the experimental comparison also tested an adapter module (following the same strategy reported in [20]) based on a FiLM layer that is tuned for each task in order to remap features. The paper refers to this approach as Adapt.

TABLE III  
AUC (%) / EER(%) FOR MIA ATTACKS ON DIFFERENT CONFIGURATIONS. PERFORMANCES ARE DIVIDED INTO STEPS, WHERE THE DATA RELATED TO EACH TASK ARE REPORTED. BEST AND SECOND BEST RESULTS ARE HIGHLIGHTED IN BLUE.

|       | Replay | Step 1    | Step 2    |           |           | Step 3    |           |           | Step 4    |           |           |  |
|-------|--------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|--|
|       |        | Task1     | Task1     | Task2     | Task1     | Task2     | Task3     | Task1     | Task2     | Task3     | Task4     |  |
| Std.  | 0 %    | 56.8/31.5 | 56.0/18.4 | 50.5/28.2 | 56.9/24.1 | 50.5/45.2 | 54.3/47.8 | 57.0/21.2 | 57.8/45.0 | 53.9/38.8 | 54.9/34.2 |  |
|       | 10%    | 57.3/31.5 | 55.6/19.4 | 49.7/13.7 | 56.3/26.3 | 52.7/39.8 | 51.1/48.1 | 55.2/21.5 | 60.8/45.0 | 54.1/47.0 | 53.5/43.0 |  |
|       | 30%    | 56.0/31.5 | 55.5/26.4 | 51.8/37.6 | 56.5/30.9 | 53.6/47.0 | 54.3/43.3 | 54.7/37.0 | 57.4/42.6 | 52.2/47.1 | 51.4/48.2 |  |
| Adapt | 0 %    | 56.9/34.7 | 54.9/46.6 | 48.0/33.7 | 54.0/48.3 | 51.9/30.1 | 52.4/35.1 | 54.9/46.8 | 50.5/32.7 | 50.6/32.6 | 50.8/33.4 |  |
|       | 10%    | 57.4/37.0 | 57.4/45.0 | 49.9/27.1 | 55.8/45.9 | 49.4/26.0 | 54.6/35.7 | 56.5/45.4 | 49.6/41.1 | 51.0/43.5 | 52.8/44.0 |  |
|       | 30%    | 57.2/32.9 | 54.5/47.6 | 49.8/29.1 | 54.4/47.9 | 48.7/35.3 | 48.8/49.7 | 53.3/48.4 | 48.5/48.4 | 50.1/49.8 | 49.8/49.5 |  |
| CDML  | 0 %    | 49.0/49.6 | 50.1/49.6 | 49.0/48.5 | 49.4/49.3 | 50.3/49.6 | 51.3/48.8 | 49.8/48.8 | 49.5/49.1 | 52.4/48.2 | 51.2/48.7 |  |
|       | 10%    | 48.5/48.5 | 47.6/49.0 | 50.6/48.5 | 48.4/48.3 | 50.8/49.6 | 49.4/48.5 | 50.8/49.6 | 51.4/45.6 | 51.4/48.6 | 50.7/49.1 |  |
|       | 30%    | 49.8/49.7 | 48.4/49.0 | 49.0/48.8 | 51.2/48.7 | 50.5/49.9 | 54.0/47.8 | 52.1/49.2 | 53.0/48.0 | 50.6/49.1 | 47.7/48.5 |  |

The CDML setting assumes that each task  $k$  is associated with a modulating code  $s_k$  which is transmitted to the next stages. In order to correctly-classify a sample, users must know the correct modulation code  $s_k$ , otherwise they can apply a random guessing or use a constant modulation.

Performance is evaluated measuring classification accuracy (to evaluate the impact of forgetting) and of Area Under Curve (AUC) and the Equal Error Rate (EER) from ROC curves whenever considering the efficiency of a MIA attack (AUC needs to be as close as possible to 50 %, while EER is to be maximized).

## B. Results

At first, the impact of catastrophic forgetting was evaluated across the different steps for different strategies. In the experimental validation, tests compared a standard fine-tuning (labeled *Std.*), strengthened by replay with different percentages of repetition (see Fig. 4). The CDML approach permits mitigating the accuracy loss without requiring data retransmission and reprocessing since accuracy is comparable to the one obtained with replay methods. As for *Adapt* approach, similar consideration can be done although in this case the average performance is lower since the number of trainable parameters increases, thus requiring more data and computational complexity.

Note also that minimal replay can be adopted for CDML as well, thus maximizing the final performance without requiring a significant retransmission (10 %). Another advantage of CDML lies in reduced accuracy variance across the different tasks (vertical bars of the graph): the use of CDML layer permits smoothing the accuracy throughout the different subsets, while in the standard set-up values depend on the processing order.

Tests also verified that the robustness to inference attacks is compromised by replaying. Table III reports the Area Under Curve (AUC) and the Equal Error Rate (EER) for the ROC curves associated to MIA attacks under different CL configurations. It is possible to notice in many *Std.* set-ups the attack is successful (error lower than 40 %), and the adoption of random replay somehow mitigates the inference since more data are processed by the network, and therefore, overfitting is somehow reduced.

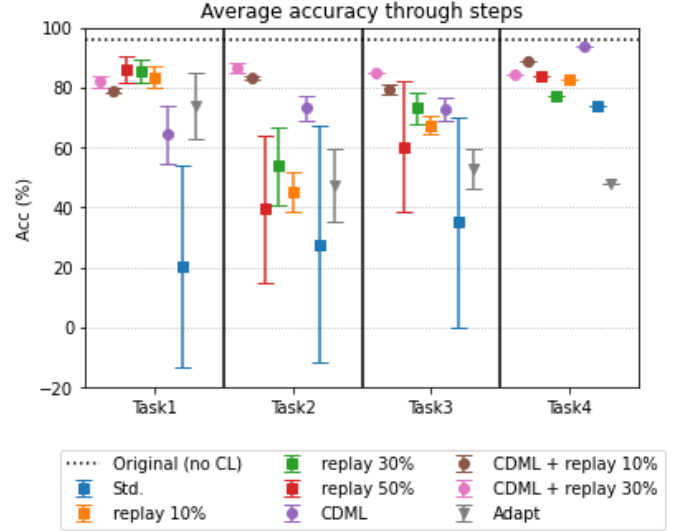


Fig. 4. Average classification accuracy for different CL methods across the different steps. Vertical bars denote accuracy variance across different training sets. Dashed line relates to architecture in [18], while solid lines are related to the proposed CDML-based approach and Adapt.

On the other side, the proposed solution (CDML) permits improving the situation since EER values are lifted up to uncertainty (50 %) for all the CDML solutions. Indeed, Table III shows that the CDML solution obtained the best (dark blue cells) or the second best (light blue cells) performance among all the possible configuration on each task. Notice that EER is always higher than 48 % in all configurations. The table also reports the value of *Adapt* approach as well. Notice this second strategy works as well, but significant parameter transmission is required. Indeed, weights and biases  $\gamma_k, \beta_k$  require the additional transmission of 16384 bytes for each task  $k$ , while CDML approach requires communicating 4 bytes only (i.e., the size of seed value for sequence generation).

## Ablation studies

In order to verify the impact of replaying, different runs were performed varying the percentage of data re-processed from the previous tasks. Fig. 4 shows accuracy values obtained with 10 %, 30 %, and 50 % of data replayed, while Table III reports values with no replay, 10 %, and 30 % of replay data: as the percentage increases, vulnerability slightly decreases since

more data are processed by the network. As for modulating solutions (CDML, Adapt), high percentages do not change either accuracy or attack success percentages significantly, and therefore, replay can therefore be constrained.

## V. DISCUSSION AND FINAL CONCLUSIONS

The paper presented a continual learning strategy for class-incremental gait identification systems where embedding features are modulated by means of a Code Division Modulation Layer (CDML). This unit scrambles the generated features according to multiple pseudo-random binary sequences associated to each task. In this way, it is possible to mitigate catastrophic forgetting since latent representations are more uniformly distributed in the feature space. This advantage can be obtained with null or minimal replay thus minimizing the computational cost and privacy leakage. Moreover, the use of a modulating code mitigates membership inference attacks under the considered black-box setting since attackers need to know in advance the associated code. At the same time, it is possible to enable different levels of privacy since different users may be enabled in the recognition of different subsets of enrolled subjects.

Future investigations will be devoted to testing more complex attacks and verifying the accuracy of the protection mechanism on other biometric traces (e.g., faces or irises) and using more complex identification networks (like transformer-based detector, or systems using low-rank adaptation to combat catastrophic forgetting). Moreover, experiments will evaluate the effectiveness of the approach in a dataset-incremental continual learning scheme, where acquisition conditions and the characteristics of samples may vary.

## REFERENCES

- [1] B. Zhao, S. Tang, D. Chen, H. Bilen, and R. Zhao, "Continual representation learning for biometric identification," *WACV*, 2021.
- [2] F. Rahman, M. Schiemer, A. R. Sanabria, and J. Ye, "Continual learning in sensor-based human activity recognition with dynamic mixture of experts," *Pervasive and Mobile Computing*, vol. 110, p. 102044, 2025. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1574119225000331>
- [3] V. D. Katkar, R. Mandal, U. Biswas, M. Lunagaria, G. G. Tejjani, and S. J. Mousavirad, "Enhancing biometric authentication privacy and security: A synergistic approach using cancelable biometrics and federated learning," *Alexandria Engineering Journal*, vol. 135, pp. 36–63, 2026. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1110016825011895>
- [4] A. F. Baig, S. Eskeland, and B. Yang, "Privacy-preserving continuous authentication using behavioral biometrics," *Int. J. Inf. Secur.*, vol. 22, p. 1833–1847, 2023.
- [5] D. Li, N. Huang, Z. Wang, and H. Yang, "Personalized federated continual learning for task-incremental biometrics," *IEEE Internet of Things Journal*, vol. 10, no. 23, pp. 20776–20788, 2023.
- [6] A. Hassanpour, M. Moradikia, B. Yang, A. Abdelhadi, C. Busch, and J. Fierrez, "Differential privacy preservation in robust continual learning," *IEEE Access*, vol. 10, pp. 1–1, 01 2022.
- [7] H.-S. Park, H.-C. Chu, M.-K. Sung, C. Kim, J. Lee, D.-W. Kim, and J. Lee, "Survey on replay-based continual learning and empirical validation on feasibility in diverse edge devices using a representative method," *Mathematics*, vol. 13, no. 14, 2025. [Online]. Available: <https://www.mdpi.com/2227-7390/13/14/2257>
- [8] E. Camuffo and S. Milani, "Continual learning for lidar semantic segmentation: Class-incremental and coarse-to-fine strategies on sparse data," *2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pp. 2447–2456, 2023. [Online]. Available: <https://api.semanticscholar.org/CorpusID:258048943>
- [9] E. Perez, F. Strub, H. de Vries, V. Dumoulin, and A. Courville, "Film: visual reasoning with a general conditioning layer," in *Proceedings of the Thirty-Second AAAI Conference on Artificial Intelligence and Thirtieth Innovative Applications of Artificial Intelligence Conference and Eighth AAAI Symposium on Educational Advances in Artificial Intelligence*, ser. AAAI'18/IAAI'18/EAAI'18. AAAI Press, 2018.
- [10] N. Loo, S. Swaroop, and R. E. Turner, "Combining variational continual learning with fiLM layers," in *4th Lifelong Machine Learning Workshop at ICML 2020*, 2020. [Online]. Available: <https://openreview.net/forum?id=fZBEGA1d-4Y>
- [11] J. Liang, J. Zhong, H. Gu, Z. Lu, X. Tang, G. Dai, S. Huang, L. Fan, and Q. Yang, "Diffusion-driven data replay: A novel approach to combat forgetting in federated class continual learning," in *ECCV*, 2024.
- [12] J. Niu, P. Liu, X. Zhu, K. Shen, Y. Wang, H. Chi, Y. Shen, X. Jiang, J. Ma, and Y. Zhang, "A survey on membership inference attacks and defenses in machine learning," *Journal of Information and Intelligence*, vol. 2, no. 5, pp. 404–454, 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2949715924000064>
- [13] M. Nasr, R. Shokri, and A. Houmansadr, "Comprehensive privacy analysis of deep learning: Stand-alone and federated learning under passive and active white-box inference attacks," *ArXiv*, vol. abs/1812.00910, 2018. [Online]. Available: <https://api.semanticscholar.org/CorpusID:54444175>
- [14] N. Carlini, S. Chien, M. Nasr, S. Song, A. Terzis, and F. Tramèr, "Membership inference attacks from first principles," in *2022 IEEE Symposium on Security and Privacy (SP)*, 2022, pp. 1897–1914.
- [15] S. Yeom, I. Giacomelli, M. Fredrikson, and S. Jha, "Privacy risk in machine learning: Analyzing the connection to overfitting," *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*, pp. 268–282, 2017. [Online]. Available: <https://api.semanticscholar.org/CorpusID:2656445>
- [16] S. Cavašin, D. Mari, S. Milani, and M. Conti, "Fingerprint membership and identity inference against generative adversarial networks," *Pattern Recognition Letters*, vol. 185, pp. 184–189, 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167865524002216>
- [17] D. DeAlcala, A. Morales, J. Fierrez, G. Mancera, R. Tolosana, and J. Ortega-Garcia, "Is my data in your ai? membership inference test (mint) applied to face biometrics," *IEEE Access*, vol. 13, pp. 163 805–163 819, 2025.
- [18] Q. Zou, Y. Wang, Q. Wang, Y. Zhao, and Q. Li, "Deep learning-based gait recognition using smartphones in the wild," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3197–3212, 2020.
- [19] G. Agnetti, A. Migliorati, D. Mari, T. Bianchi, S. Milani, and E. Magli, "Ternary neural networks for gait identification in wearable devices," in *2024 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2024, pp. 1–6.
- [20] J. Wang, S. Zhang, X. Wei, and S. Tian, "Gaitadapt: Continual learning for evolving gait recognition," *ArXiv*, vol. abs/2508.03375, 2025. [Online]. Available: <https://api.semanticscholar.org/CorpusID:280526810>
- [21] R. C. Magel and S. H. Wibowo, "Comparing the powers of the wald-wolfowitz and kolmogorov-smirnov tests," *Biometrical Journal*, vol. 39, no. 6, pp. 665–668, 1997.
- [22] M. Hénon, "A two-dimensional mapping with a strange attractor," *The theory of chaotic attractors*, pp. 94–102, 2004.
- [23] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no. 5560, pp. 459–467, 1976.
- [24] T. Yoshida, H. Mori, and H. Shigematsu, "Analytic study of chaos of the tent map: band structures, power spectra, and critical behaviors," *Journal of statistical physics*, vol. 31, pp. 279–308, 1983.
- [25] G. L. Steele Jr and S. Vigna, "Computationally easy, spectrally good multipliers for congruential pseudorandom number generators," *Software: Practice and Experience*, vol. 52, no. 2, pp. 443–458, 2022.