Yongduan Song
Chongqing University, CHINA

Dongrui Wu
Huazhong University of Science and Technology, CHINA

Carlos A. Coello Coello
CINVESTAV-IPN, MEXICO

Georgios N. Yannakakis
University of Malta, MALTA

Huajin Tang
Zhejiang University, CHINA

Yiu-ming Cheung
Hong Kong Baptist University, HONG KONG

Hussein Abbass
University of New South Wales, AUSTRALIA

CIS Publication Spotlight

IEEE Transactions on Neural Networks and Learning Systems

A Gradient-Guided Evolutionary Approach to Training Deep Neural Networks, by S. Yang, Y. Tian, C. He, X. Zhang, K. C. Tan, and Y. Jin, *IEEE Transactions on Neural Networks and Learning Systems*, Vol. 33, No. 9, Sep. 2022, pp. 4861–4875.

Digital Object Identifier: 10.1109/TNNLS.2021.3061630

"It has been widely recognized that the efficient training of neural networks (NNs) is crucial to classification performance. While a series of gradient-based approaches have been extensively developed, they are criticized for the ease of trapping into local optima and sensitivity to hyperparameters. Due to the high robustness and wide applicability, evolutionary algorithms (EAs) have been regarded as a promising alternative for training NNs in recent years. However, EAs suffer from the curse of dimensionality and are inefficient in training deep NNs (DNNs). By inheriting the advantages of both the gradient-based approaches and EAs, this article proposes a gradient-guided evolutionary approach to train DNNs. The proposed approach suggests a novel genetic operator to optimize the weights in the search space, where the search direction is determined by the gradient of weights. Moreover, the network sparsity is considered in the proposed approach, which highly reduces the network complexity and alleviates overfitting. Experimental results on single-layer NNs, deep-layer NNs, recurrent NNs, and convolutional NNs (CNNs) demonstrate the effectiveness of the proposed approach. In short, this work not only introduces a novel approach for training DNNs but also enhances the performance of EAs in solving large-scale optimization problems."

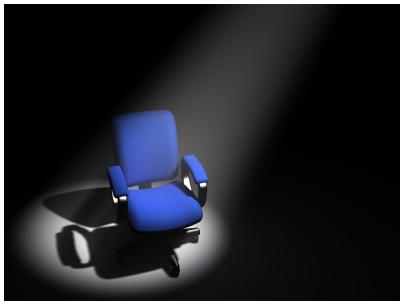

IMAGE LICENSED BY INGRAM PUBLISHING

IEEE Transactions on Fuzzy Systems

Multiclass Fuzzily Weighted Adaptive-Boosting-Based Self-Organizing Fuzzy Inference Ensemble Systems for Classification, by X. Gu and P. P. Angelov, *IEEE Transactions on Fuzzy Systems*, Vol. 30, No. 9, Sep. 2022, pp. 3722–3735.

Digital Object Identifier: 10.1109/TFUZZ.2021.3126116

"Adaptive boosting (AdaBoost) is a widely used technique to construct a stronger ensemble classifier by combining a set of weaker ones. Zero-order fuzzy inference systems (FISs) are very powerful prototype-based predictive models for classification, offering both great prediction precision and high user interpretability. However, the use of zero-order FISs as base classifiers in AdaBoost has not been explored yet. To bridge the gap, in this article, a novel multiclass fuzzily weighted AdaBoost

Digital Object Identifier 10.1109/MCI.2022.3223500
Date of current version: 13 January 2023

(FWAdaBoost)-based ensemble system with a self-organizing fuzzy inference system (SOFIS) as the ensemble component is proposed. To better incorporate the SOFIS, FWAdaBoost utilizes the confidence scores produced by the SOFIS in both sample weight updating and ensemble output generation, resulting in more accurate classification boundaries and greater prediction precision. Numerical examples on a wide range of benchmark classification problems demonstrate the efficacy of the proposed approach."

Fuzzy Rule Interpolation With K-Neighbors for TSK Models, by P. Zhang, C. Shang, and Q. Shen, *IEEE Transactions on Fuzzy Systems*, Vol. 30, No. 10, Oct 2022, pp. 4031–4043.

Digital Object Identifier: 10.1109/TFUZZ.2021.3136359

"When a fuzzy system is presented with an incomplete (or sparse) rule base, fuzzy rule interpolation (FRI) offers a useful mechanism to infer conclusions for unmatched observations. However, most existing FRI methodologies are established for Mamdani inference models, but not for Takagi–Sugeno–Kang (TSK) ones. This article presents a novel approach for computing interpolated outcomes with TSK models, using only a small number of neighboring rules to an unmatched observation. Compared with existing methods, the new approach helps improve the computational efficiency of the overall interpolative reasoning process, while minimizing the adverse impact on accuracy induced by firing those rules of low similarities with the new observation. For problems that involve a rule base of a large size, where closest neighboring rules may be rather alike to one another, a rule-clustering-based method is introduced. It derives an interpolated conclusion by first clustering rules into different groups with a clustering algorithm and then, by utilizing only those rules that are each selected from one of a given, small number of closest rule clusters. Systematic experimental examinations are carried out to verify the efficacy of the introduced techniques, in comparison with state-of-the-art methods, over a range of benchmark regression problems, while employing different clustering algorithms (which also shows the flexibility in ways of implementing the novel approach)."

IEEE Transactions on Evolutionary Computation

An Approximated Gradient Sign Method Using Differential Evolution for Black-Box Adversarial Attacks, by C. Li, H. Wang, J. Zhang, W. Yao, and T. Jiang, *IEEE Transactions on Evolutionary Computation*, Vol. 26, No. 5, Oct. 2022, pp. 976–990.

Digital Object Identifier: 10.1109/TEVC.2022.3151373

"Recent studies show that deep neural networks are vulnerable to adversarial attacks in the form of subtle perturbations to the input image, which leads the model to output wrong prediction. Such an attack can easily succeed by the existing white-box attack methods, where the perturbation is calculated based on the gradient of the target network. Unfortunately, the gradient is often unavailable in the real-world scenarios, which makes the black-box adversarial attack problems practical and challenging. In fact, they can be formulated as high-dimensional black-box optimization problems at the pixel level. Although evolutionary algorithms are well known for solving black-box optimization problems, they cannot efficiently deal with the high-dimensional decision space. Therefore, we propose an approximated gradient sign method using differential evolution (DE) for solving black-box adversarial attack problems. Unlike most existing methods, it is novel that the proposed method searches the gradient sign rather than the perturbation by a DE algorithm. Also, we transform the pixel-based decision space into a dimension-reduced decision space by combining the pixel differences from the input image to neighbor images, and two different techniques for selecting neighbor images are introduced to build the transferred decision space. In addition, six variants of the proposed method are designed according to the different neighborhood selection and optimization search strategies. Finally, the performance of the proposed method is compared with a number of the state-of-the-art adversarial attack algorithms on CIFAR-10 and ImageNet datasets. The experimental results suggest that the proposed method shows superior performance for solving black-box adversarial attack problems, especially nontargeted attack problems."

IEEE Transactions on Games

Beyond Genre: Classifying Virtual Reality Experiences, by M. Foxman, D. Beyea, A. P. Leith, R. A. Ratan, V. H. H. Chen and B. Klebig, *IEEE Transactions on Games*, Vol. 14, No. 3, Sep. 2022, pp. 466–477.

Digital Object Identifier: 10.1109/TG.2021.3119521

"Because virtual reality (VR) shares common features with video games, consumer content is usually classified according to traditional game genres and standards. However, VR offers different experiences based on the medium's unique affordances. To account for this disparity, the article presents a comparative analysis of titles from the Steam digital store across three platform types: VR only, VR supported, and non-VR. We analyzed data from a subset of the most popular applications within each category ($N = 141$, 93, and 1217, respectively). The three classification types we analyzed were academic game genres, developer defined categories, and user-denoted tags. Results identify the most common content classifications (e.g., Action and Shooter within VR only applications), the relative availability of each between platforms (e.g., Casual is more common

in VR only than VR supported or non-VR), general platform popularity (e.g., VR only received less positive ratings than VR supported and non-VR), and which content types are associated with higher user ratings across platforms (e.g., Action and Music/Rhythm are most positively rated in VR only). Our findings ultimately provide a foundational framework for future theoretical constructions of classification systems based on content, market, interactivity, sociality, and service dependencies, which underlay how consumer VR is currently categorized."

IEEE Transactions on Cognitive and Developmental Systems

An End-to-End Spiking Neural Network Platform for Edge Robotics: From Event-Cameras to Central Pattern Generation, by A. Lele, Y. Fang, J. Ting, and A. Raychowdhury, *IEEE Transactions on Cognitive and Developmental Systems*, Vol. 14, No. 3, Sep. 2022, pp. 1092–1103.

Digital Object Identifier: 10.1109/TCDS.2021.3097675

"Learning to adapt one's gait with environmental changes plays an essential role in the locomotion of legged robots which remains challenging for constrained computing resources and energy budget, as in the case of edge-robots. Recent advances in bio-inspired vision with dynamic vision sensors (DVSs) and associated neuromorphic processing can provide promising solutions for end-to-end sensing, cognition, and control tasks. However, such bio-mimetic closed-loop robotic systems based on event-based visual sensing and actuation in the form of spiking neural networks (SNNs) have not been well explored. In this work, we program the weights of a bio-mimetic multigait central pattern generator (CPG) and couple it with DVS-based visual data processing to show a spike-only closed-loop robotic system for a prey-tracking scenario. We first propose a supervised learning rule based on stochastic weight updates to produce a multigait producing spiking-CPG (SCPG) for hexapod robot locomotion. We then actuate the SCPG to seamlessly transition between the gaits for a nearest prey tracking task by incorporating SNN-based visual processing for input event-data generated by the DVS. This for the first time, demonstrates the natural coupling of event data flow from event-camera through SNN and neuromorphic locomotion. Thus, we exploit bio-mimetic dynamics and energy advantages of spike-based processing for autonomous edge-robotics."

IEEE Transactions on Emerging Topics in Computational Intelligence

ES Attack: Model Stealing Against Deep Neural Networks Without Data Hurdles, by X. Yuan, L. Ding, L. Zhang, X. Li, and D. O. Wu, *IEEE Transactions on Emerging Topics in Computational Intelligence*, Vol. 6, No. 5, Oct. 2022, pp. 1258–1270.

Digital Object Identifier: 10.1109/TETCI.2022.3147508

"Deep neural networks (DNNs) have become the essential components for various commercialized machine learning services, such as Machine Learning as a Service (MLaaS). Recent studies show that machine learning services face severe privacy threats - well-trained DNNs owned by MLaaS providers can be stolen through public APIs, namely model stealing attacks. However, most existing works undervalued the impact of such attacks, where a successful attack has to acquire confidential training data or auxiliary data regarding the victim DNN. In this paper, we propose ES Attack, a novel model stealing attack without any data hurdles. By using heuristically generated synthetic data, ES Attack iteratively trains a substitute model and eventually achieves a functionally equivalent copy of the victim DNN. The experimental results reveal the severity of ES Attack: i) ES Attack successfully steals the victim model without data hurdles, and ES Attack even outperforms most existing model stealing attacks using auxiliary data in terms of model accuracy; ii) most countermeasures are ineffective in defending ES Attack; iii) ES Attack facilitates further attacks relying on the stolen model."

IEEE Transactions on Artificial Intelligence

Smoothed Generalized Dirichlet: A Novel Count-Data Model for Detecting Emotional States, by F. Najar and N. Bouguila, *IEEE Transactions on Artificial Intelligence*, Vol. 3, No. 5, Oct. 2022, pp. 685–698.

Digital Object Identifier: 10.1109/TAI.2021.3120043

"In this article, we propose novel approaches to deal with the problem of burstiness, the challenge of count-data sparseness, and the curse of dimensionality. We introduce a smoothed generalized Dirichlet distribution that is a smoothed variant of the generalized Dirichlet distribution and a generalization of the smoothed Dirichlet. We provide different learning methods based on mixture models and agglomerative clustering-based geometrical information: Kullback–Leibler divergence, Fisher metric, and Bhattacharyya distance. Moreover, we show that the new smoothed generalized Dirichlet could be considered as a prior to the multinomial, which generates a new distribution for count data that we call the smoothed generalized Dirichlet multinomial. In particular, we present an approximation based on Taylor series expansion for better performance and optimized running time in the case of high-dimensional count data. The proposed models are evaluated through two emotion detection applications: disaster-tweet-related emotions and pain intensity estimation. Experiments show the efficiency and the robustness of our approaches when dealing with texts, videos, and images."