Haibo He, Jon Garibaldi, Kay Chen Tan, Julian Togelius, Yaochu Jin, and Yew Soon Ong

Publication Spotlight

# CIS Publication Spotlight

## *IEEE Transactions on Neural Networks and Learning Systems*

*Adversarial Examples: Attacks and Defenses for Deep Learning*, by X. Yuan, P. He, Q. Zhu, and X. Li, *IEEE Transactions on Neural Networks and Learning Systems*, Vol. 30, No. 9, September 2019, pp. 2805–2824.

Digital Object Identifier: 10.1109/TNNLS.2018.2886017

"With rapid progress and significant successes in a wide spectrum of applications, deep learning is being applied in many safety-critical environments. However, deep neural networks (DNNs) have been recently found vulnerable to well-designed input samples called adversarial examples. Adversarial perturbations are imperceptible to human but can easily fool DNNs in the testing/deploying stage. The vulnerability to adversarial examples becomes one of the major risks for applying DNNs in safety-critical environments. Therefore, attacks and defenses on adversarial examples draw great attention. In this paper, we review recent findings on adversarial examples for DNNs, summarize the methods for generating adversarial examples, and propose a taxonomy of these methods. Under the taxonomy, applications for adversarial examples are investigated. We further elaborate on countermeasures for adversarial examples. In addition, three major challenges in adversarial examples and the potential solutions are discussed."

IN THE FRAME/©DIGITAL VISION

*Object Detection With Deep Learning: A Review*, by Z. Zhao, P. Zheng, S. Xu, and X. Wu, *IEEE Transactions on Neural Networks and Learning Systems*, Vol. 30, No. 11, November 2019, pp. 3212–3232.

Digital Object Identifier: 10.1109/TNNLS.2018.2876865

"Due to object detection's close relationship with video analysis and image understanding, it has attracted much research attention in recent years. Traditional object detection methods are built on handcrafted features and shallow trainable architectures. Their performance easily stagnates by constructing complex ensembles that combine multiple low-level image features with high-level context from object detectors and scene classifiers. With the rapid development in deep learning, more powerful tools, which are able to learn semantic, high-level, deeper features, are introduced to address the problems existing in traditional architectures. These models behave differently in network architecture, training strategy, and optimization function. In this paper, we provide a review of deep learning-based object detection frameworks. Our review begins with a brief introduction on the history of deep learning and its representative tool, namely, the convolutional neural network. Then, we focus on typical generic object detection architectures along with some modifications and useful tricks to improve detection performance further. As distinct specific detection tasks exhibit different characteristics, we also briefly survey several specific tasks, including salient object detection, face detection, and pedestrian detection. Experimental analyses are also provided to compare various methods and draw some meaningful conclusions. Finally, several promising directions and tasks are provided to serve as guidelines for future work in both object detection and relevant neural network-based learning systems."

## *IEEE Transactions on Fuzzy Systems*

*PALM: An Incremental Construction of Hyperplanes for Data Stream Regression*, by M. M. Ferdaus, M. Pratama, S. G. Anavatti, and M. A. Garratt, *IEEE Transactions on Fuzzy Systems*, Vol. 27, No. 11, November 2019, pp. 2115–2129.

*Digital Object Identifier 10.1109/MCI.2020.2976181*
*Date of current version: 10 April 2020*

Digital Object Identifier: 10.1109/TFUZZ.2019.2893565

"Data stream has been the underlying challenge in the age of big data because it calls for real time data processing with the absence of a retraining process and/or an iterative learning approach. In the realm of the fuzzy system community, data stream is handled by algorithmic development of self-adaptive neuro-fuzzy systems (SANFS) characterized by the single-pass learning mode and the open structure property that enables effective handling of fast and rapidly changing natures of data streams. The underlying bottleneck of SANFSs lies in its design principle, which involves a high number of free parameters (rule premise and rule consequent) to be adapted in the training process. This figure can even double in the case of the type-2 fuzzy system. In this paper, a novel SANFS, namely parsimonious learning machine (PALM), is proposed. PALM features utilization of a new type of fuzzy rule based on the concept of hyperplane clustering, which significantly reduces the number of network parameters because it has no rule premise parameters. PALM is proposed in both type-1 and type-2 fuzzy systems where all of which characterize a fully dynamic rule-based system. That is, it is capable of automatically generating, merging, and tuning the hyperplane-based fuzzy rule in the single-pass manner. Moreover, an extension of PALM, namely recurrent PALM, is proposed and adopts the concept of teacher-forcing mechanism in the deep learning literature. The efficacy of PALM has been evaluated through numerical study with six real-world and synthetic data streams from public database and the authors' own real-world project of autonomous vehicles. The proposed model showcases significant improvements in terms of computational complexity and number of required parameters against several renowned SANFSs, while attaining comparable and often better predictive accuracy."

*Fuzzy Support Vector Machine With Relative Density Information for Classifying Imbalanced Data*, by H. YU, C. Sun, X. Yang, S. Zheng and H. Zou, *IEEE Transactions on Fuzzy Systems*, Vol. 27, No. 12, December 2019, pp. 2353–2367.

Digital Object Identifier: 10.1109/TFUZZ.2019.2898371

"Fuzzy support vector machine (FSVM) has been combined with class imbalance learning (CIL) strategies to address the problem of classifying skewed data. However, the existing approaches hold several inherent drawbacks, causing the inaccurate prior data distribution estimation, further decreasing the quality of the classification model. To solve this problem, the authors present a more robust prior data distribution information extraction method named relative density, and two novel FSVM-CIL algorithms based on the relative density information in this paper. In their proposed algorithms, a K-nearest neighbors-based probability density estimation (KNN-PDE) alike strategy is utilized to calculate the relative density of each training instance. In particular, the relative density is irrelevant with the dimensionality of data distribution in feature space, but only reflects the significance of each instance within its class; hence, it is more robust than the absolute distance information. In addition, the relative density can better seize the prior data distribution information, no matter the data distribution is easy or complex. Even for the data with small injunctions or a large class overlap, the relative density information can reflect its details well. The authors evaluated the proposed algorithms on an amount of synthetic and real-world imbalanced datasets. The results show that their proposed algorithms obviously outperform to some previous work, especially on those datasets with sophisticated distributions."

## IEEE Transactions on Evolutionary Computation

*Evolutionary Generative Adversarial Networks*, by C. Wang, C. Xu, X. Yao, and D. Tao, *IEEE Transactions on Evolutionary Computation*, Vol. 23, No. 6, December 2019, pp. 921–934.

Digital Object Identifier: 10.1109/TEVC.2019.2895748

"Generative adversarial networks (GANs) have been effective for learning generative models for real-world data. However, accompanied with the generative tasks becoming more and more challenging, existing GANs (GAN and its variants) tend to suffer from different training problems such as instability and mode collapse. This paper proposes a novel GAN framework called evolutionary GANs (E-GANs) for stable GAN training and improved generative performance. Unlike existing GANs, which employ a predefined adversarial objective function alternately training a generator and a discriminator, it evolves a population of generators to play the adversarial game with the discriminator. Different adversarial training objectives are employed as mutation operations and each individual (i.e., generator candidature) are updated based on these mutations. Then, it devises an evaluation mechanism to measure the quality and diversity of generated samples, such that only well-performing generator(s) are preserved and used for further training. In this way, E-GAN overcomes the limitations of an individual adversarial training objective and always preserves the well-performing offspring, contributing to progress in, and the success of GANs. Experiments on several datasets demonstrate that E-GAN achieves convincing generative performance and reduces the training problems inherent in existing GANs."

## IEEE Transactions on Games

*The ASC-Inclusion Perceptual Serious Gaming Platform for Autistic Children*, by E. Marchi, B. Schuller, A. Baird, S. Baron-Cohen, A. Lassalle, H. O'Reilly, D. Pigat, P. Robinson, I. Davies, T. Baltrusaitis, A. Adams, M. Mahmoud, O. Golan, S. Fridenson-Hayo, S. Tal, S. Newman, N. Meir-Goren, A. Camurri, S. Piana, S. Bolte, M. Sezgin, N. Alyuz, A. Rynkiewicz,

and A. Baranger, *IEEE Transactions on Games*, Vol. 11, No. 4, December 2019, pp. 328–339.

Digital Object Identifier: 10.1109/TG.2018.2864640

"“Serious games" are becoming extremely relevant to individuals who have specific needs, such as children with an autism spectrum condition (ASC). Often, individuals with an ASC have difficulties in interpreting verbal and nonverbal communication cues during social interactions. The ASC-Inclusion EU-FP7 funded project aims to provide children who have an ASC with a platform to learn emotion expression and recognition, through play in the virtual world. In particular, the ASC-Inclusion platform focuses on the expression of emotion via facial, vocal, and bodily gestures. The platform combines multiple analysis tools, using onboard microphone and webcam capabilities. The platform utilizes these capabilities via training games, text-based communication, animations, video, and audio clips. This paper introduces current findings and evaluations of the ASC-Inclusion platform and provides detailed description for the different modalities."

### *IEEE Transactions on Cognitive and Developmental Systems*

*Symbol Emergence in Cognitive Developmental Systems: A Survey*, by T. Taniguchi, E. Ugur, M. Hoffmann, L. Jamone, T. Nagai, B. Rosman, T. Matsuka, N. Iwahashi, E. Oztop, J. Piater, and F. Wörgötter, *IEEE Transactions on Cognitive and Developmental Systems*, Vol. 12, No. 4, December 2019, pp. 494–516.

Digital Object Identifier: 10.1109/TCDS.2018.2867772

"Humans use signs, e.g., sentences in a spoken language, for communication and thought. Hence, symbol systems like language are crucial for our communication with other agents and adaptation to our real-world environment. The symbol systems we use in our human society adaptively and dynamically change over time. In the context of artificial intelligence (AI) and cognitive systems, the symbol grounding problem has been regarded as one of the central problems related to symbols. However, the symbol grounding problem was originally posed to connect symbolic AI and sensorimotor information and did not consider many interdisciplinary phenomena in human communication and dynamic symbol systems in our society, which semiotics considered. In this paper, the authors focus on the symbol emergence problem, addressing not only cognitive dynamics but also the dynamics of symbol systems in society, rather than the symbol grounding problem. The authors first introduce the notion of a symbol in semiotics from the humanities, to leave the very narrow idea of symbols in symbolic AI. Furthermore, over the years, it became more and more clear that symbol emergence has to be regarded as a multifaceted problem. Therefore, second, the authors review the history of the symbol emergence problem in different fields, including both biological and artificial systems, showing their mutual relations. The authors summarize the discussion and provide an integrative viewpoint and comprehensive overview of symbol emergence in cognitive systems. Additionally, the authors describe the challenges facing the creation of cognitive systems that can be part of symbol emergence systems."

### *IEEE Transactions on Emerging Topics in Computational Intelligence*

*Well-M$^3$N: A Maximum-Margin Approach to Unsupervised Structured Prediction*, by S. Abidi, M. Piccardi, I. W. Tsang, and M. A. William, *IEEE Transactions on Emerging Topics in Computational Intelligence,* Vol. 3, No. 6, December 2019, pp. 427–439.

Digital Object Identifier: 10.1109/TETCI.2018.2876524

"Unsupervised structured prediction is of fundamental importance for the clustering and classification of unannotated structured data. To date, its most common approach still relies on the use of structural probabilistic models and the expectation maximization (EM) algorithm. Conversely, structural maximum-margin approaches, despite their extensive success in supervised and semi-supervised classification, have not raised equivalent attention in the unsupervised case. For this reason, in this paper, we propose a novel approach that extends the maximum-margin Markov networks (M$^3$N) to an unsupervised training framework. The main contributions of our extension are new formulations for the feature map and loss function of M$^3$N that decouple the labels from the measurements and support multiple ground-truth training. Experiments on two challenging segmentation datasets have achieved competitive accuracy and generalization compared to other unsupervised algorithms such as k-means, EM and unsupervised structural SVM, and comparable performance to a contemporary deep learning-based approach."