ABSTRACT

Deep Neural Networks (DNNs) are best known for being the state-of-the-art in artificial intelligence (AI) applications including natural language processing (NLP), speech processing, computer vision, etc. In spite of all recent achievements of deep learning, it has yet to achieve semantic learning required to reason about the data. This lack of reasoning is partially imputed to the boorish memorization of patterns and curves from millions of training samples and ignoring the spatiotemporal relationships. The proposed framework puts forward a novel approach based on variational autoencoders (VAEs) by using the potential outcomes model and developing the counterfactual autoencoders. The proposed framework transforms any sort of multimedia input distributions to a meaningful latent space while giving more control over how the latent space is created. This allows us to model data that is better suited to answer inference-based queries, which is very valuable in reasoning-based AI applications.

1. INTRODUCTION

Often in real-world applications such as multimedia, NLP, and medicine, large quantities of unlabeled data are generated every day. This surge in data gives rise to the challenging semantic gap problem (Lin, Shyu & Chen, 2012; Chen, Lin & Shyu, 2012; Zhu & Shyu, 2015; Sadiq, Yan, Shyu, Chen & Ishwaran, 2016) which is to reduce the gap between high level semantic concepts and their low level
features (Sadiq, Tao, Yan & Shyu, 2017a; Sadiq, Zmieva, Shyu & Chen, 2018; Yan, Chen, Sadiq & Shyu, 2017). Despite rigorous research endeavors, this remains one of the most challenging problems in information sciences where we have overwhelming quantities of all sorts of fast, complex, heterogeneous and unstructured data. To handle such data, conventionally we have been utilizing descriptive models that try to find deterministic features and build probabilistic models (Chen & Kashyap, 1997; Chen, 2010; Lin, Shyu & Chen, 2013; Sadiq et al., 2017b). However, the problem with discriminative models is that they, generally, estimate a hyperplane. For example, when categorizing images of cats and dogs, data points on one side of the hyperplane are categorized as cats and everything on the other side as dogs. Discriminative models follow a condition in logistic regression that relaxes the computation of a joint probability $p(x, y)$ to a conditional probability $p(x|y)$ which is much easier to calculate because it maps directly to the hyperplane that divides between two clusters. This problem gets exacerbated in deep learning models due to the increase in dimensionality and boorish memorization of patterns. Mere rotations or color-inversions in the trained images can easily confound very deep neural networks even though the modified images share the same semantics and structures as the original images (Hosseini & Poovendran, 2017).

Recently, there has been a growing concern of this shortcoming, resulting in a soaring interest in Knowledge Representation and Reasoning (KRR) (Liu, 2017) and reasoning based deep learning (Andreas, Rohrbach, Darrell & Klein, 2016; Santoro et al., 2017). We believe that the next generation of AI systems will need to have the ability to understand problems at a deeper level rather than just based on memorization of data. However, discriminative models fail completely in inferencing problems because they do not capture the underlying relationships in the input space. Figure 1 shows how the addition of an adversarial noise can completely fool the classification while the L2 loss between the original and modified images was minimal. The discriminative models considered them as identical images while producing completely different results. All images were classified with 99.9% confidence.

*Figure 1. Classification results produced by state-of-the-art deep learning models, but fooled by simple noising up of the images (Nguyen, Yosinski & Clune, 2015)*