Abstract

In this talk, I will first review the Product Quantization (PQ) and its variants developed in the area of vector quantization which has been extensively studied in information theory. In a modern large scale image retrieval system, PQ based approximate nearest neighbor (ANN) search methods have achieved high search quality and low storage overhead. Moreover, deep product quantization network combines the powerful features extraction ability and back-propagation process to obtain a better codewords of PQ. However, we then show that deep product quantization network is vulnerable to input with small and maliciously designed perturbations (a.k.a., adversarial examples). Specifically, we propose product quantization adversarial generation (PQ-AG), a simple yet effective method to generate adversarial examples for product quantization based retrieval systems. PQ-AG aims to generate imperceptible adversarial perturbations for query images to form adversarial queries, whose nearest neighbors from a targeted product quantizaiton model are not semantically related to those from the original queries. Extensive experiments show that our PQ-AQ successfully creates adversarial examples to mislead targeted product quantization retrieval models. Besides, we found that our PQ-AG significantly degrades retrieval performance in both white-box and black-box settings.