24th International Conference on Neural Information Processing (ICONIP 2017)
November 14-18, 2017
Guangzhou, China

ICONIP 2017: Paper 17482 Confirmation

Please print this confirmation page for future reference. You should receive an e-mail confirmation of your submission. **If you do not receive an e-mail notification within 24 hours, please contact ICONIP 2017 <iconip2017@foxmail.com>.**

Dear Author(s),

Your paper number 17482 was resubmitted successfully to ICONIP 2017. Please use the paper number in all your correspondence. In case of problems with your PDF file you will be notified and asked to resubmit a corrected file.

Your submission was recorded as follows:

Title: Effectiveness of adversarial inputs on class-imbalanced convolutional neural networks
Author(s): Rafael Possas and Ying Zhou
Affiliation(s):
University of Sydney, Australia
University of Sydney, Australia
Email: rafael.possas@sydney.edu.au, ying.zhou@sydney.edu.au

Abstract:
Convolutional neural networks (CNNs) performance has increased considerably in the last couple of years. However, as with most machine learning methods, these networks suffer from the data imbalance problem - when the underlying training dataset is comprised of an unequal number of samples for each label/class. Such imbalance enforces a phenomena known as domain shift that causes the model to have poor generalisation when presented with previously unseen data. Recent research has focused on a technique called gradient sign that intensifies domain shift in CNNs by modifying inputs to deliberately yield erroneous model outputs, while appearing unmodified to human observers. Several commercial systems rely on image recognition techniques to perform well. Therefore, adversarial attacks poses serious threats to their integrity. In this work we present an experimental study that sheds light on the link between adversarial attacks, imbalanced learning and transfer learning. Through a series of experiments we evaluate the fast gradient sign method on class imbalanced CNNs, linking model vulnerabilities to the characteristics of its underlying training set and internal model knowledge.

Preferred form of presentation: Oral

Paper Topics:
A03. Deep neural networks
A05. Computer vision

Student Paper: Yes

If you need to update your submission again please go to:

http://sci-review.com/iconip2017/upload.php?PaperID=17482

On this page you will need to use the following password:

q3psu6gt9

For the latest news and announcements, please visit the conference's home page:

http://www.iconip2017.org

All inquiries should be sent to ICONIP 2017 <iconip2017@foxmail.com>.

Thank you for your submission.

Sincerely,
ICONIP 2017 <iconip2017@foxmail.com>
ICONIP 2017 Program Chair

Home

Processed: 2017-06-19 01:05:05 EDT.