Alhussein Fawzi

CONTACT INFORMATION

E-mail: hussein.fawzi@gmail.com
Mobile: +1 (424) 345-5119
WWW: www.alhusseinfawzi.info

RESEARCH INTERESTS

Robust classification, computer vision, classification invariance, signal and image processing.

EMPLOYMENT

Postdoctoral fellow, UCLA Vision Lab. – Los Angeles, USA *01/2017 - ongoing*
Host: Prof. Stefano Soatto.

EDUCATION

Ecole Polytechnique Fédérale de Lausanne – Lausanne, Switzerland *May 2012 - Dec 2016*
PhD in Electrical Engineering.

- Dissertation title: *Robust image classification: analysis and applications.*
- Research in the robustness of state-of-the-art image classification methods to perturbations in the data; invariance of classification to geometric transformations.
- Supervisor: Prof. Pascal Frossard. Thesis committee: Prof. Joan Bruna (UC Berkeley), Dr. François Fleuret (IDIAP Research Institute), Prof. Nikos Paragios (Ecole Centrale Paris), Prof. Pierre Vandergheynst (EPFL).

Ecole Polytechnique Fédérale de Lausanne – Lausanne, Switzerland *Sept 2010 - Feb 2012*
M.Sc. in Electronics and Electrical Engineering (Information Technologies orientation)

- Dissertation title: *Geometric group sparsity in image analysis.*
- Awarded best Master's student in Electronics and Electrical Engineering.

Ecole Centrale de Nantes – Nantes, France *Sept 2008 - Aug 2010*
Diplôme d'Ingénieur (equivalent to B.Sc).

Classes préparatoires aux Grandes Ecoles (CPGE), Lycée Chaptal – Paris, France *2006 - 2008*
Concentration in Mathematics and Physics.

AWARDS

- Awarded SNSF "Early Postdoctoral Mobility" grant to go to UCLA Vision Lab. Starting January 2017.
- Recipient twice of the IBM PhD Fellowship award (Academic years 2013-2014 and 2015-2016).
- SIA Vaudoise prize for student excellence (October 2012).
- Anna Barbara Reinhard Prize for student excellence from the Institution of Engineering and Technology (IET) (October 2012).
- Gold medal in Egyptian Olympiad in Informatics (EOI) 2004.

PUBLICATIONS

2017 and pre-prints

▷ S-M. Moosavi-Dezfooli*, **A. Fawzi***, O. Fawzi, P. Frossard, *Universal adversarial perturbations*, IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2017. (*: Equal contribution).
Oral presentation.
Demo on YouTube.
Neural Networks Have A Universal Flaw, I-Programmer, 04/11/2016.
Universal adversarial perturbations, HackerNews, 29/10/2016.

▷ **A. Fawzi**, O. Fawzi, P. Frossard, *Analysis of classifiers' robustness to adversarial perturbations*, submitted to Machine Learning Journal.

2016

Journal articles:

▷ **A. Fawzi**, M. Sinn, P. Frossard, *Multi-task additive models with shared transfer functions*, IEEE Transactions on Signal Processing, 2016.

▷ **A. Fawzi**, J-B. Fiot, B. Chen, M. Sinn, P. Frossard, *Structured Dimensionality Reduction for Additive Model Regression*, IEEE Transactions on Data Knowledge and Engineering (TKDE), 2016.

Peer-reviewed conferences:

▷ **A. Fawzi***, S-M. Moosavi-Dezfooli*, P. Frossard, *Robustness of classifiers: from adversarial to random noise*, Neural Information Processing Systems (NIPS), 2016. (*: Equal contribution).

▷ **A. Fawzi**, P. Frossard, *Measuring the effect of nuisance variables on classifiers*, British Machine Vision Conference (BMVC), 2016. **Oral presentation**

▷ S-M. Moosavi-Dezfooli, **A. Fawzi**, P. Frossard, *DeepFool: a simple and accurate method to fool deep neural networks*, IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016.

▷ **A. Fawzi**, H. Samulowitz, D. Turaga, P. Frossard, *Adaptive data augmentation for image classification*, International Conference on Image Processing (ICIP), 2016.

▷ **A. Fawzi**, H. Samulowitz, D. Turaga, P. Frossard, *Image inpainting through neural networks hallucinations*, Image, Video and Multidimensional Signal Processing Workshop (IVMSP), 2016.

2015

Journal articles:

▷ **A. Fawzi**, M. Davies, P. Frossard, *Dictionary learning for fast classification based on soft-thresholding*, International Journal of Computer Vision (IJCV), 114(2-3), pp.306-321, 2015.

Peer-reviewed conferences:

▷ **A. Fawzi**, P. Frossard, *Manitest: Are classifiers really invariant?*, British Machine Vision Conference (BMVC), 2015. Matlab and C++ code available on project webpage.

▷ **A. Fawzi**, O. Fawzi, P. Frossard, *Fundamental limits on adversarial robustness*, ICML Deep Learning Workshop, 2015.

2014 and before

Journal articles:

▷ **A. Fawzi**, P. Frossard, *Image registration with sparse approximations in parametric dictionaries*, SIAM J. on Imaging Sci., 6(4), pp. 2370-2403, 2013.

Peer-reviewed conferences:

▷ **A. Fawzi**, P. Frossard, *Classification of unions of subspaces with sparse representations*, Asilomar Conference on Signals, Systems and Computers, 2013. *(Invited paper).*

▷ **A. Fawzi**, P. Frossard, *A geometric framework for registration of sparse images*, IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2013.

▷ **A. Fawzi**, P. Frossard, *Thresholding-based reconstruction of compressed correlated signals*, IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2012.

Work and research experience

PhD research

▷ *Robust image classification: analysis and applications* *05/2012 - 12/2016*

In the past decade, image classification systems have witnessed major advances that led to record performances on challenging datasets. However, little is known about the behavior of these classifiers when the data is subject to perturbations, such as random noise, structured geometric transformations, and other common nuisances (e.g., occlusions and illumination changes). We study in this thesis fundamental limitations on the reliability of state-of-the-art image classifiers, and provide tools to empirically assess their robustness to perturbations.

Internship IBM Thomas J. Watson Research Center *09/2015 - 12/2015*

▷ *Enhancing the robustness of classifiers using automatic data augmentation schemes*

Data augmentation is the process of generating samples by transforming training data, with the target of improving the accuracy and robustness of classifiers. Data augmentation is however an art, as it involves

many manual choices. We propose an automated and principled way for finding transformation parameters that lead to increased accuracy and robustness of classifiers. We show that in cases where training data is insufficient, the new training algorithm yields significant improvements in robustness and accuracy.

Internship IBM Research Dublin *02/2014 - 06/2014*

▷ *Multi-task additive models with shared transfer functions*
Additive models are a popular class of interpretable regression models that represent the relation between covariates and response variables as the sum of low-dimensional transfer functions. In this project, we develop a framework that extends additive regression models to multi-task scenarios, with multiple response variables. Assuming that unknown correlations exist between the different tasks, we propose an algorithm to detect such correlations, and learn a global model for the tasks. We show applications of the proposed framework for the forecasting of electric load data measured by smart meters.

▷ *Structured dimensionality reduction for additive models*
In many large-scale forecasting problems, thousands of covariates, such as temperatures at different weather stations, are available. Fitting a model in this scenario is challenging as the model can hardly be *interpreted* by field experts, and tends to *overfit* the data. We introduce a constrained model that addresses these two issues, and we propose a principled fitting algorithm based on novel optimization techniques. We show applications of our method in electric load forecasting and bike prediction problems.

Invited talks

- *Universal adversarial perturbations*, 29th of November 2016.
  Department of Computer Science, University of Bristol.
  Host: Prof. Dima Damen.
- *Are classifiers really robust to deformations in the data?*, 15th of September 2016
  Xerox Research Center Europe (XRCE), Grenoble.
  Host: Dr. Gianluca Monaci.
- *Are classifiers really robust to deformations in the data?*, 6th of September 2016
  Université Catholique de Louvain (UCL), Louvain-la-Neuve, Belgium.
  Host: Prof. Laurent Jacques.
- *Are classifiers really robust to deformations in the data?*, 24th of April 2016
  Idiap Research Institute, Martigny, Switzerland.
  Host: Dr. François Fleuret.
- *Towards the design of robust classifiers and related applications*, 18th of December 2015
  IBM TJ Watson Research Center, NY, USA.
  Host: Dr. Deepak Turaga.
- *Feature selection and clustering in Generalized Additive Models (GAM)*, 3rd of June 2014.
  IBM Research Dublin, Ireland.
  Host: Dr. Olivier Verscheure.

Conferences & workshops attended

- Neural Information Processing Systems (NIPS), 2016, Barcelona, Spain.
- British Machine Vision Conference (BMVC), 2016, York, UK.
- Image, Video and Multidimensional Signal Processing Workshop (IVMSP) 2016, Bordeaux, France.
- Neural Information Processing Systems (NIPS) 2015, Montreal, Canada.
- British Machine Vision Conference (BMVC) 2015, Swansea, UK.
- International Computer Vision Summer School (ICVSS) 2015, Sicily, Italy.
- International Conference on Machine Learning (ICML) 2015, Lille, France.
- International Traveling Workshop on Interactions between Sparse models and Technology (iTwist) 2014, Namur, Belgium.
- Signal Processing with Adaptive Sparse Structured Representation (SPARS) 2013, Lausanne, Switzerland.
- ENS/INRIA Computer Vision and Machine Learning summer school (CVML) 2013, Paris, France.
- Asilomar Conference on Signals, Systems and Computers, 2013, Monterey, CA, USA.
- International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2013, Vancouver, Canada.
- International Traveling Workshop on Interactions between Sparse models and Technology (iTwist) 2012, Marseille, France.

- International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2012, Kyoto, Japan.

Service

Reviewer for
- IEEE Transactions on Signal Processing
- IEEE Transactions on Image Processing
- IEEE Signal Processing Letters
- IEEE Pattern Recognition Letters
- Elsevier Digital Signal Processing (DSP)
- IEEE Transactions on Neural Networks and Learning Systems
- IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI)
- Neural Information Processing Systems (NIPS)
- Interational Conference on Computer Vision (ICCV)

Computer Skills

Matlab, Python, C/C++, Java.

Languages

Bilingual French and Arabic
Fluent in English
Basic level in Spanish

Citizenship

French and Egyptian

Date of Birth

20/06/1989