

Vienna Deep Learning Meetup



23 April 2018 @ Wien Energie



Vienna Deep Learning Meetup



The Organizers:



Thomas Lidy
Musimap








Jan Schlüter
OFAI





Alex Schindler
AIT & TU Wien


New Youtube Channel

Suchen







 **Vienna Deep Learning Meetup**



Vienna Deep Learning Meetup
52 Abonnenten

KANAL ANPASSEN**CREATOR STUDIO**

ÜBERSICHT**VIDEOS****PLAYLISTS****KANÄLE****DISKUSSION****KANALINFO**

LIVE-STREAM tonight!

SUBSCRIBE: <http://youtube.com/ViennaDeepLearningMeetup>

ANGESAGTE KANÄLE

BELIEBTE KANÄLE AUF
YOUTUBE

Vienna 17th Deep Learning Meetup

Agenda:

- Welcome (Tom Lidy)
- Introduction (Michael Elias, Wien Energie)
- **AI to provide a bird's-eye view**
Anouk Visser, CTO - Birds.ai
- Announcements
 - *30 minutes break*
- **Enhancing the medical expert - how to help doctors with AI**
Christoph Goetz, CTO - ImageBiopsyLab
- Latest News & Hot Topics (Alex Schindler, Jan Schlüter)
- Networking and Discussions



Job Announcements

The background of the lower half of the slide is a photograph of two men in business suits. The man in the foreground, who is Black, is smiling and looking down at a laptop. The man in the background, who is white, is also looking at the laptop. Overlaid on the left side of the image is a faint, light-colored network map with nodes and connecting lines. Some of the nodes are labeled with city names: New York, London, Zürich, Paris, Singapore, Hong Kong, and Tokyo.

WE ARE HIRING
MACHINE LEARNING, DEEP LEARNING,
DATA MINING EXPERT

Andreas Burner, SmartStream Innovation Lab



About us ...

- Leading software vendor in the FinTech space
- >1,500 customers globally, 70 of the World's top 100 banks

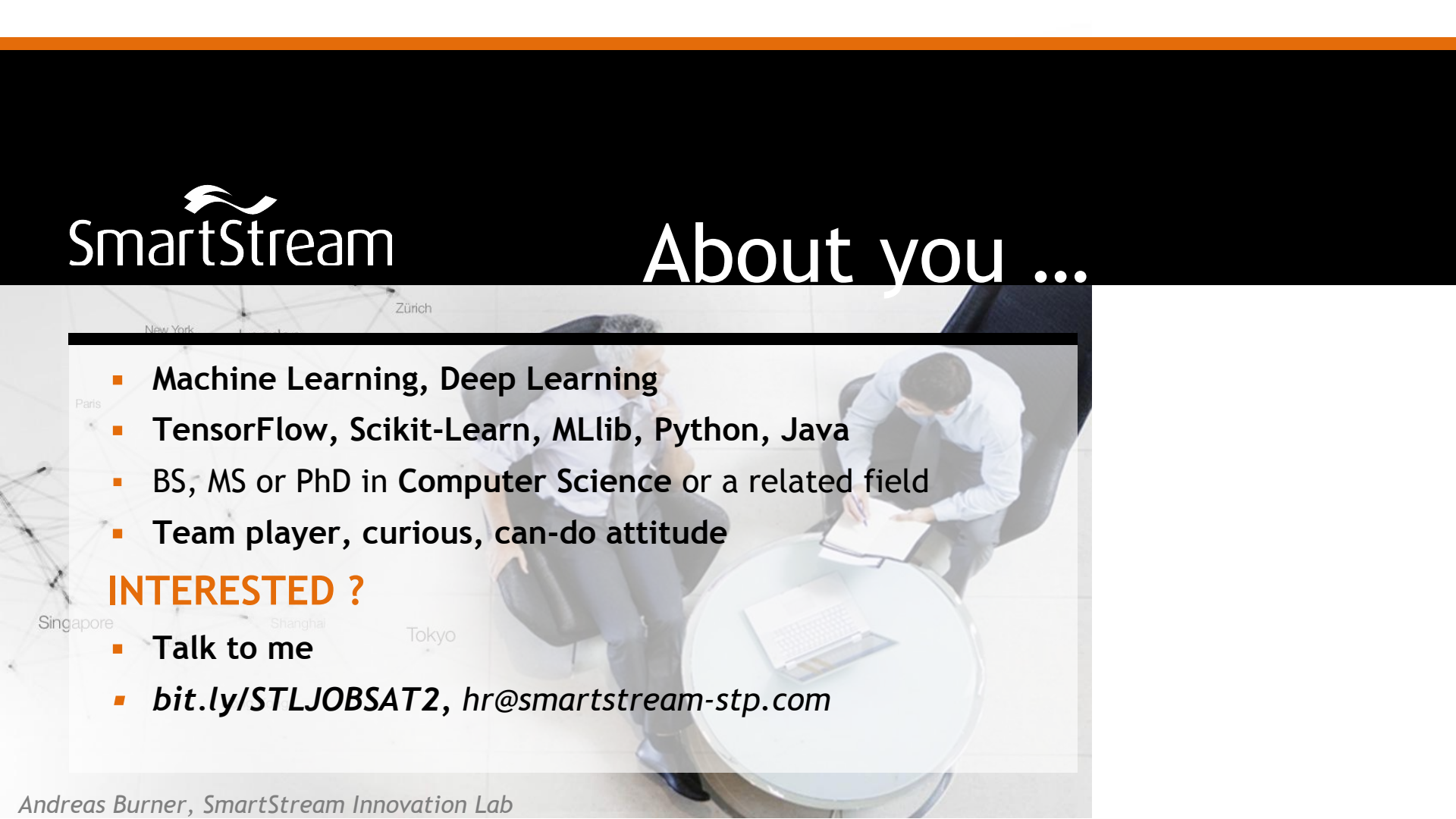
SMARTSTREAM INNOVATION LAB IN VIENNA

- Research, assess, prototype
- Incorporate ML/DL into our products
- Broad range of techniques





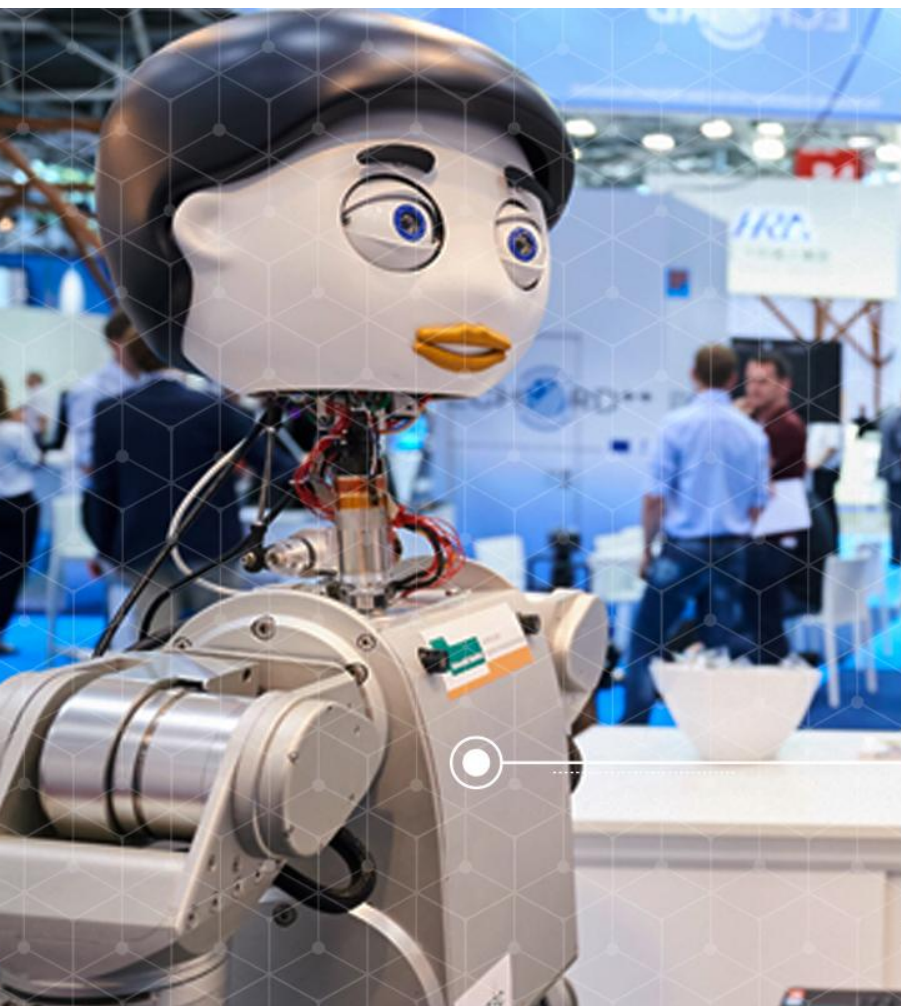
About you ...

- 
- The background of the slide is a high-angle photograph of two men in business attire sitting in modern chairs around a white circular table. One man is looking at a laptop on the table, while the other is looking at a document. The scene is set in a bright, minimalist office environment.
- Machine Learning, Deep Learning
 - TensorFlow, Scikit-Learn, MLlib, Python, Java
 - BS, MS or PhD in Computer Science or a related field
 - Team player, curious, can-do attitude

INTERESTED ?

- Talk to me
- bit.ly/STLJOBSAT2, hr@smartstream-stp.com

Event Announcements



CALLING STARTUPS!

**Exhibit at the leading trade show
for smart automation and robotics**

JOIN US!

19 - 22 JUNE / MUNICH



Ethics & Bias in Artificial Intelligence

May 7th, 2018, 18:30 - 23:00

Precht-Saal, Hauptgebäude, TU Wien

Vienna
Deep
Learning
Meetup



Deep Learning and the Crisis of Trust in Computing

Prof. Moshe Vardi, Rice University

The Big Data Illusion and its Impact on Flourishing with General AI

Prof. Sarah Spiekermann-Hoff, WU Wien

Panel Discussion “Ethics & Bias in AI”

Panelists

Prof. Moshe Vardi

Prof. Peter Purgathofer

Prof. Sarah Spiekermann-Hoff

Prof. Mark Coeckelbergh

Dr. Christof Tschohl

Rice University

TU Wien

WU Wien

Universität Wien

Research Institute Austria

Moderation

Markus Mooslechner

Terra Mater Productions

Event Registration

More information and link for registration: aiethics.cisvienna.com



Vienna 17th Deep Learning Meetup

Agenda:

- Welcome (Tom Lidy)
- Introduction (Michael Elias, Wien Energie)
- **AI to provide a bird's-eye view**
Anouk Visser, CTO - Birds.ai
- Announcements
 - *30 minutes break*
- **Enhancing the medical expert - how to help doctors with AI**
Christoph Goetz, CTO - ImageBiopsyLab
- Latest News & Hot Topics (Alex Schindler, Jan Schlüter)
- Networking and Discussions



Hot Topics & Latest News

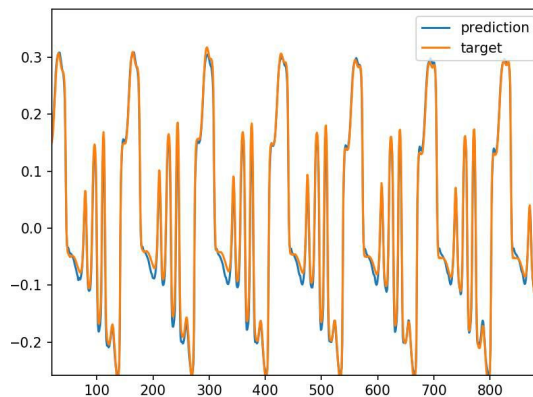
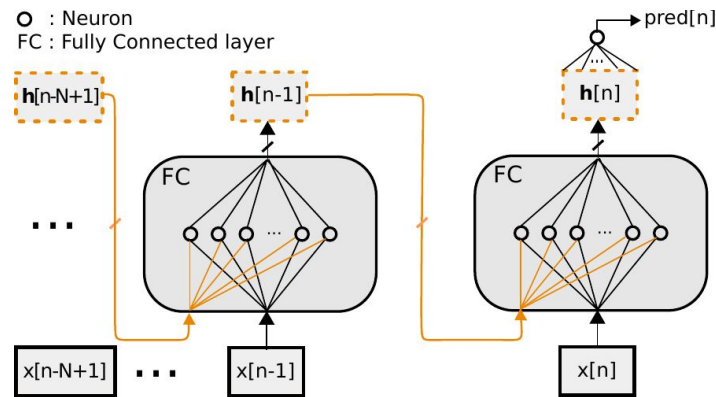
a short block at every meetup
to briefly present recent papers and news

Send us contributions (tom.lidy@gmail.com)
or come with slides to do a short block yourself!

REAL TIME EMULATION OF PARAMETRIC GUITAR TUBE AMPLIFIER WITH LONG SHORT TERM MEMORY NEURAL NETWORK

Thomas Schmitz and Jean-Jacques Embrechts¹

- Minimize Mean Squared Error (MSE) between generated sound and training signal
- 1% MSE for Engl Retro Tubes 50 **at full gain** (lot of distortions)
- Further included Amplifier parameters *Gain, Low, Middle, Treble* - also 1% MSE



DeepWriting: Making Digital Ink Editable via Deep Generative Modeling

- Handwriting recognition
- Pen-based interaction
- Handwriting Beautification
- Handwriting Synthesis
- Spell-Checking & Correction

Eighty percent of success is showing up Write

Eighty percent of success is showing up

Eighty percent of success is showing up

Eighty percent of success is showing up

A

this line in many styles

under review is
this line in many styles
but rather he wants to show the
this line in many styles
with two words to the
this line in many styles

B

The diagram illustrates the DeepWriting interface workflow. It starts with a text input field containing "I wish I could fly" and a "Write" button. An arrow points to a "TOOLBOX" containing "Select", "Analyze", "Undo Stroke", and "Clear Canvas". Another arrow points to a second "TOOLBOX" containing "Select", "Analyze", "Undo Stroke", and "Clear Canvas". The final output is a box containing the beautified handwriting "I wish I could write".

TOOLBOX

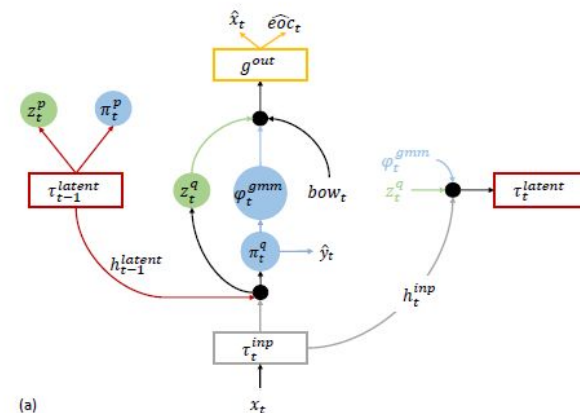
- Select
- Analyze
- Undo Stroke
- Clear Canvas

TOOLBOX

- Select
- Analyze
- Undo Stroke
- Clear Canvas

C

- Conditional Variational Recurrent Neural Network (C-VRNN)
 - introducing a set of latent random variables to
 - increase the expressive power of the model
 - Decouple style from content



DeepWriting: Examples

It's showtime folks

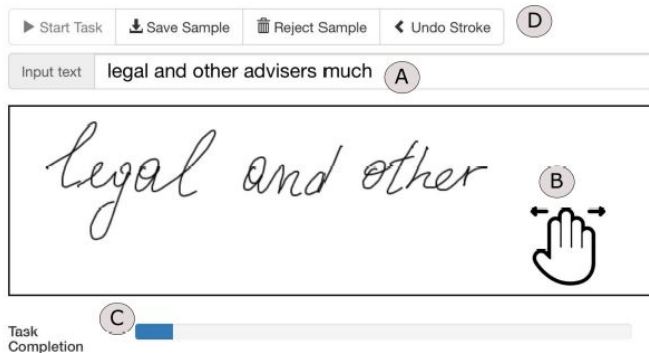
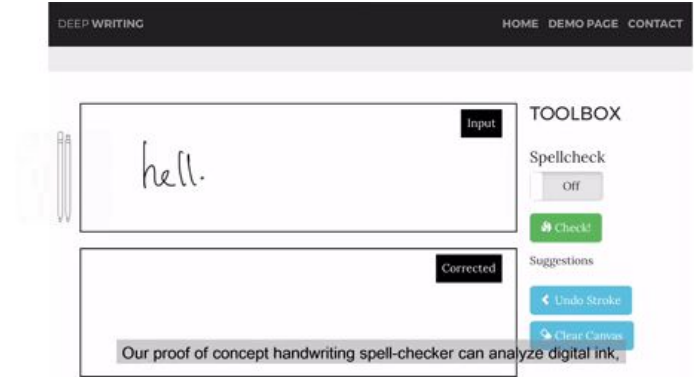


settle this argument

It's showtime folks

call up the reinforcements

It's showtime folks



Dogs vs. Cats Test

Raise your hand if you see a dog, keep it down if you see a cat

Dogs vs. Cats Test

Raise your hand if you see a dog, keep it down if you see a cat



Dogs vs. Cats Test

Raise your hand if you see a dog, keep it down if you see a cat



Dogs vs. Cats Test

Raise your hand if you see a dog, keep it down if you see a cat



Dogs vs. Cats Test

Raise your hand if you see a dog, keep it down if you see a cat



Dogs vs. Cats Test

Raise your hand if you see a dog, keep it down if you see a cat



Adversarial Examples that Fool both Human and Computer Vision

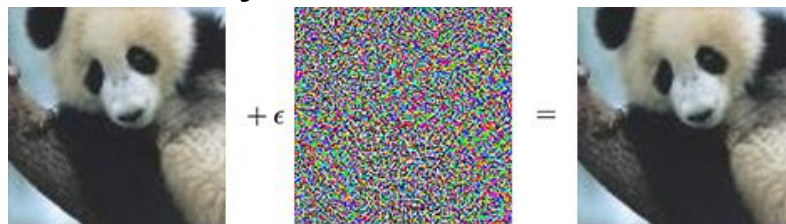
It's a cat manipulated such that multiple different CNNs think it's a dog.



At least at brief exposure, humans are tricked into making the wrong decision as well.

Adversarial Attacks Against Medical Deep Learning Systems

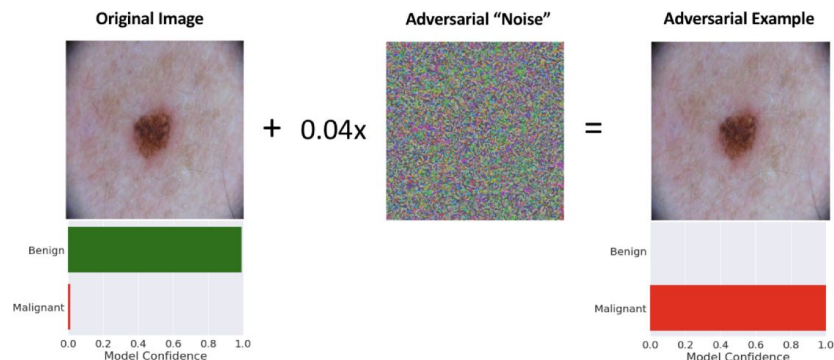
- Adversarial Example: Image manipulated to cross a classification boundary without humans noticing the change



<https://arxiv.org/abs/1412.6572>

"panda"
57.7% confidence

"gibbon"
99.3% confidence



<https://arxiv.org/abs/1802.08195>

<https://arxiv.org/abs/1802.08195>

Adversarial Attacks Against Medical Deep Learning Systems

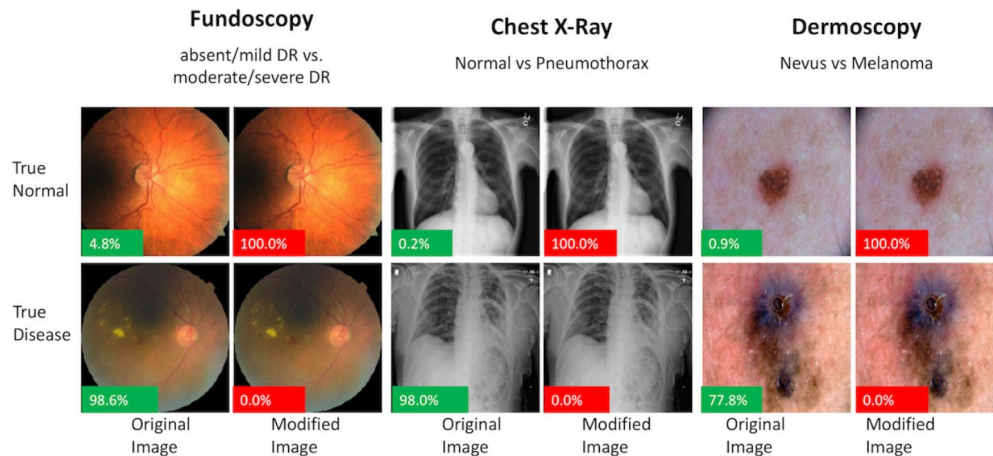
Why would you want to do that?

- US spent around \$3.3 trillion on healthcare (17.8% of GDP)
- Payments depend on diagnoses
- In the future, diagnoses will probably be confirmed by algorithms to reduce possibilities for fraud

Why is it easy to do that?

- Experts often disagree, systematic fraud is difficult to detect
- Medical imaging is highly standardized, thus easy to attack
- Hospital software infrastructure is slow to update

Adversarial Attacks Against Medical Deep Learning Systems

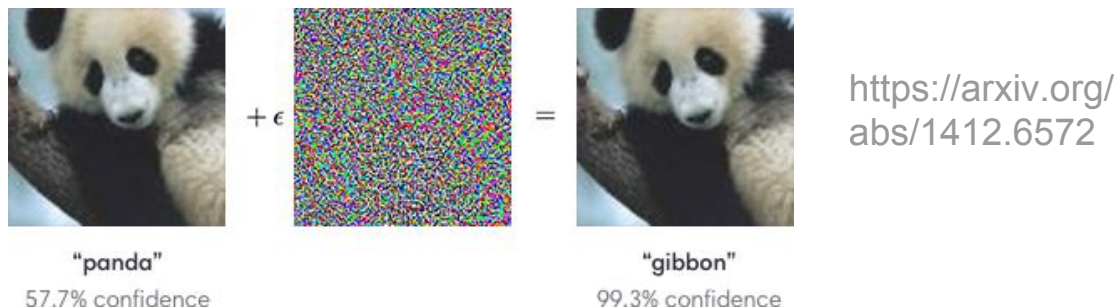


What to do about it?

- Algorithmic defenses: ongoing research
- Infrastructural defenses: have imaging devices sign the images to prevent undetected manipulations

Poison Frogs! Targeted Clean-Label Poisoning Attacks on Neural Networks

- Adversarial Example: Image manipulated to cross a classification boundary without humans noticing the change

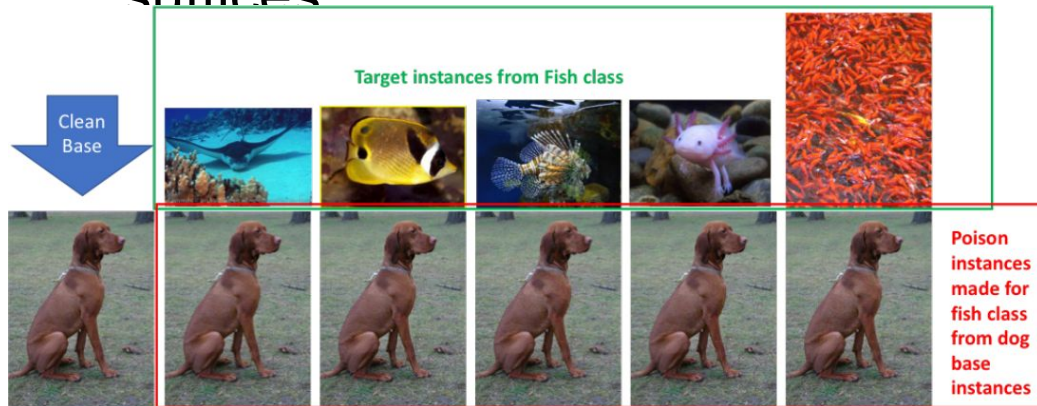


- Adding adversarials to the *training set*, we can manipulate the classification boundary that is learned
- Useful attack vector when we can create training examples for a system that will be labeled by humans

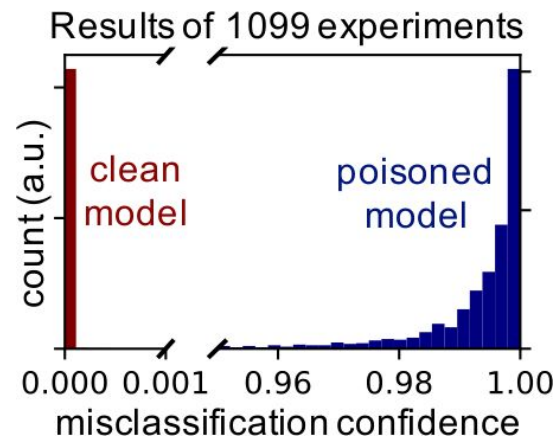
<https://arxiv.org/abs/1804.00792>

Poison Frogs! Targeted Clean-Label Poisoning Attacks on Neural Networks

- For transfer learning (tuning the last layer of a CNN pretrained on ImageNet), a single poisoned example suffices

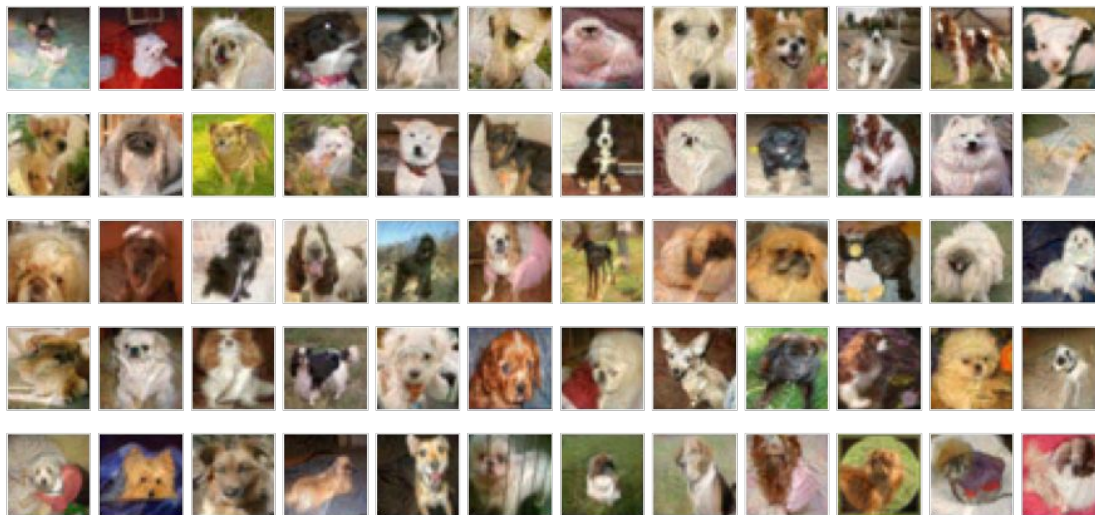


Adding one of the dog images to the training set causes the respective fish image to be misclassified with high confidence.

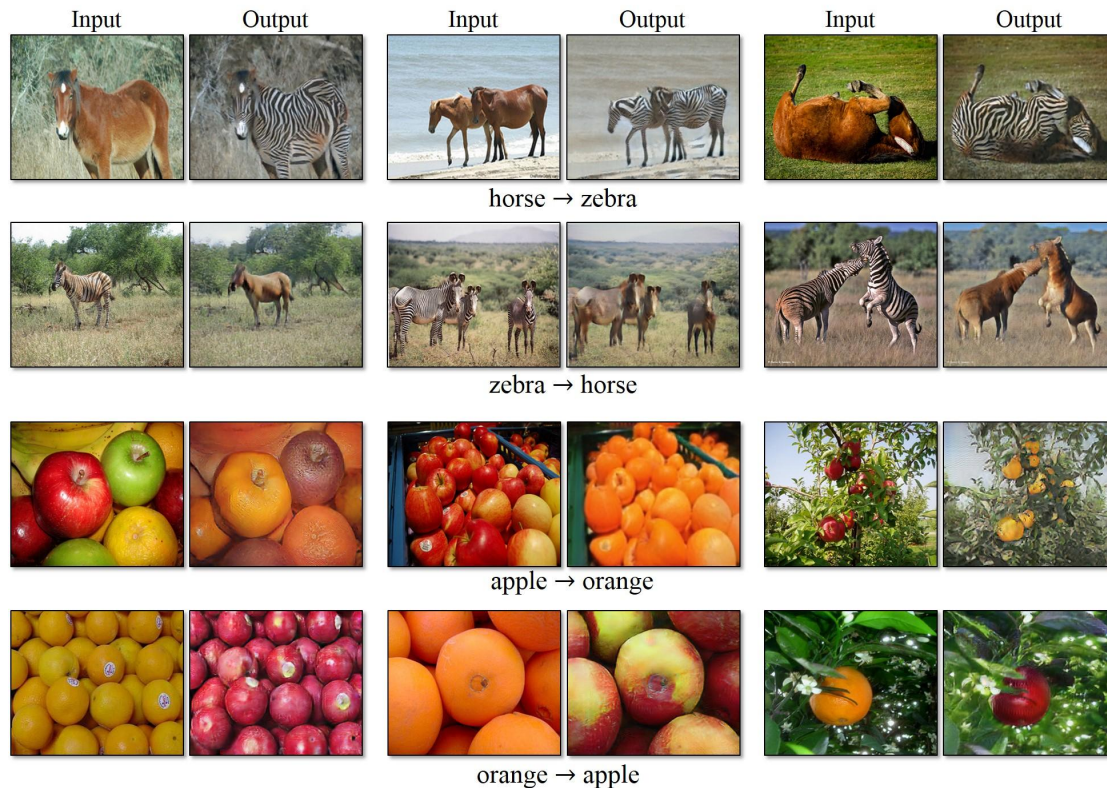


Poison Frogs! Targeted Clean-Label Poisoning Attacks on Neural Networks

- For end-to-end learning, multiple poisoned examples are required, with less elegant distortions (30% watermarking)

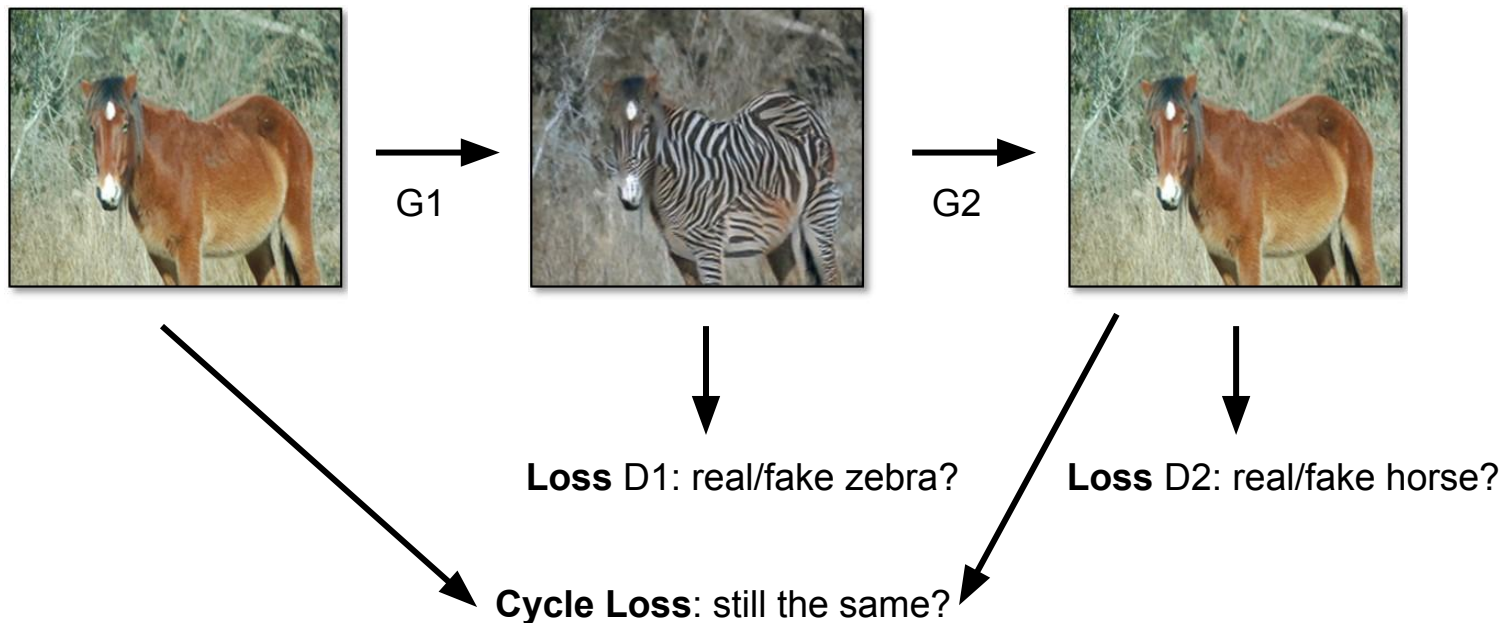


CycleGAN, a Master of Steganography

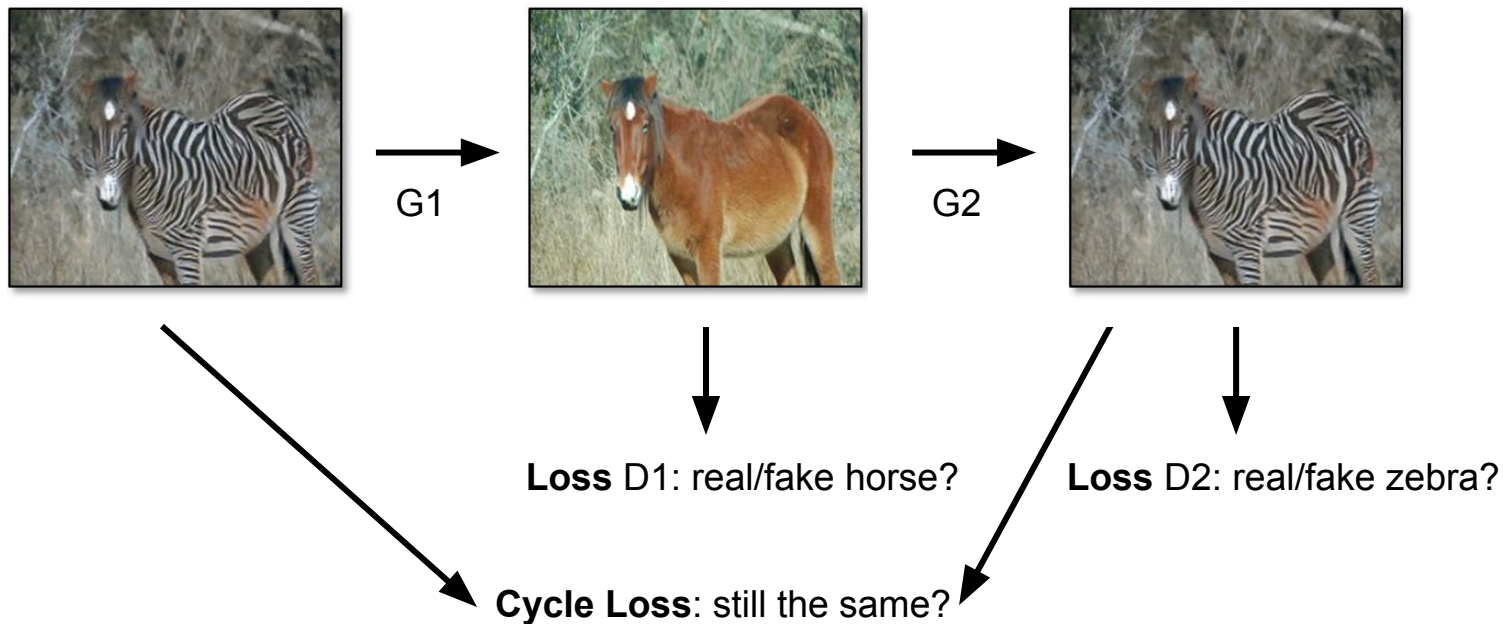


<https://arxiv.org/abs/1712.02950>

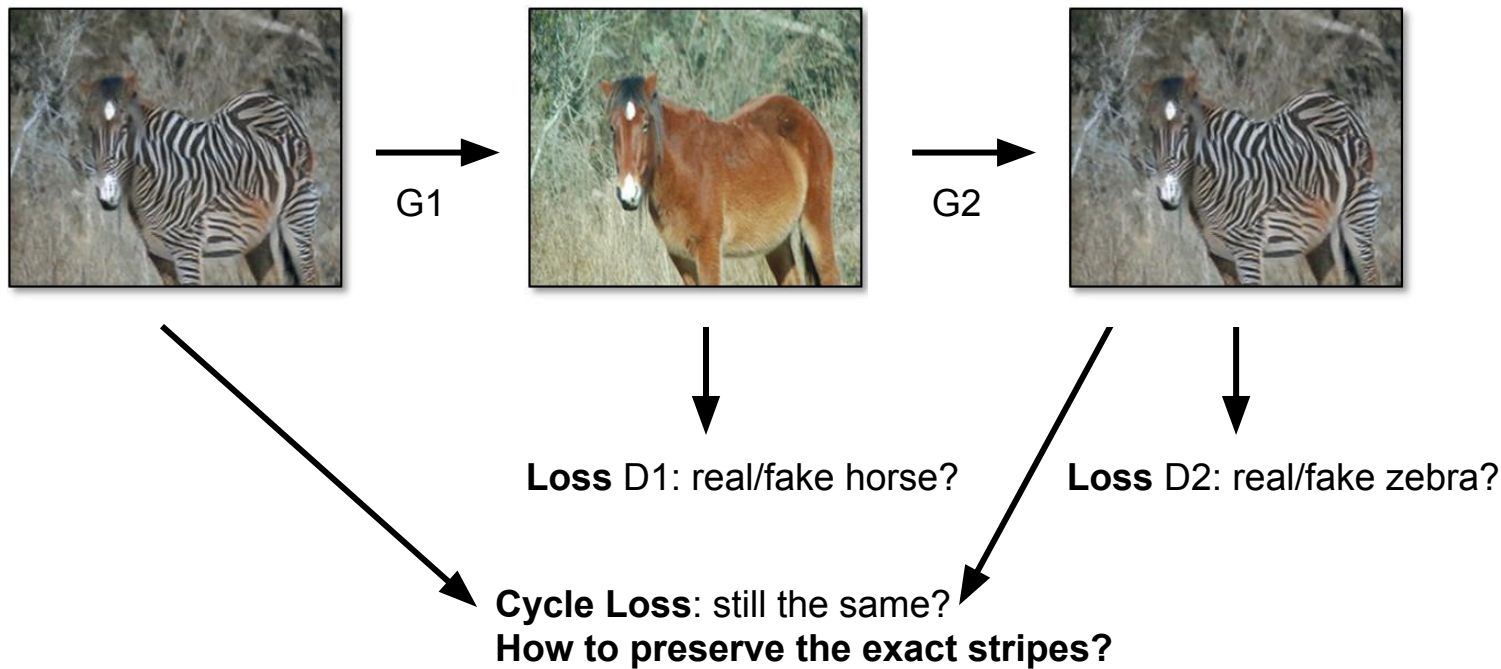
CycleGAN, a Master of Steganography



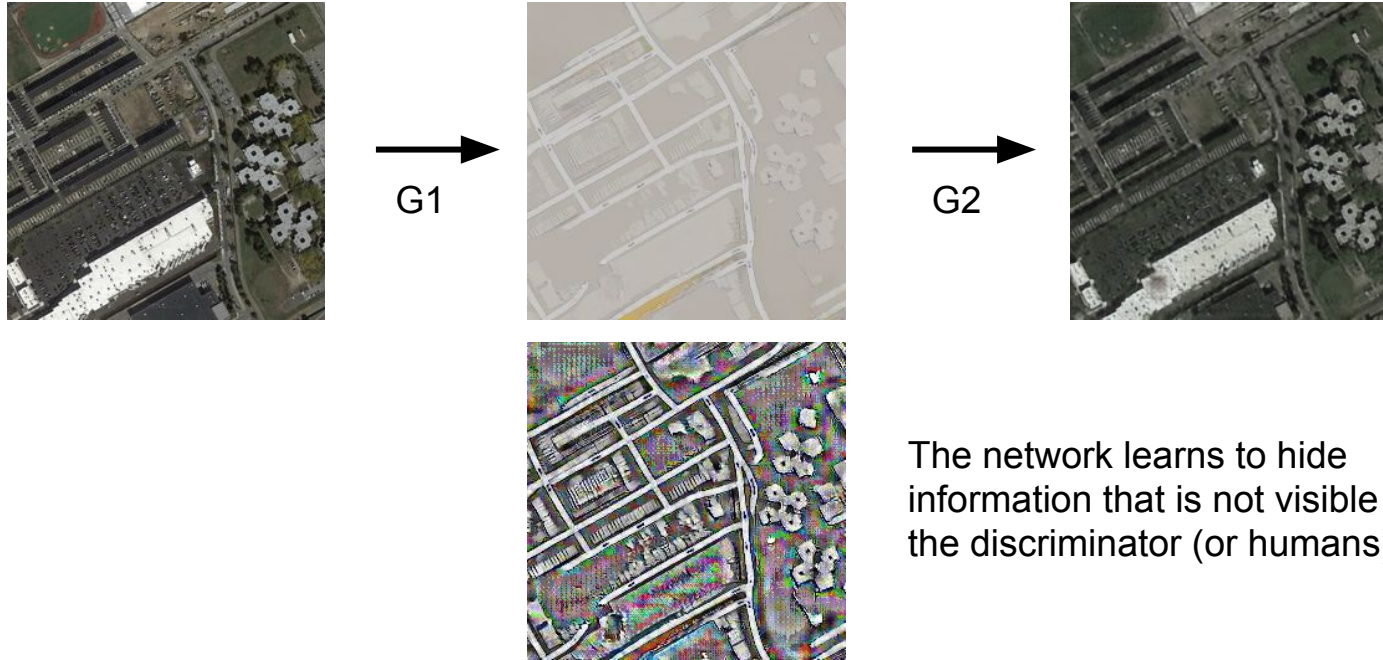
CycleGAN, a Master of Steganography



CycleGAN, a Master of Steganography



CycleGAN, a Master of Steganography



The network learns to hide information that is not visible to the the discriminator (or humans).

μ -cuDNN: Accelerating Deep Learning Frameworks with Micro-Batching

- cuDNN: NVIDIA library with deep learning primitives
- Different algorithms selected depending on available memory
- μ -cuDNN: wrapper library that splits minibatches into microbatches, so cuDNN will use a faster algorithm

Tensor Comprehensions

```
def avgpool(float(B, C, H, W) input) -> (output) {{  
    output(b, c, h, w) += input(b, c, h * {sH} + kh, w * {sW} + kw)  
    where kh in 0:{kH}, kw in 0:{kW}  
}}
```



Tensor Comprehension for 2D Average Pooling

Tons more

arxiv-sanity.com

Arxiv Sanity Preserver
Built in spare time by @karpathy to accelerate research.
Serving last 40049 papers from cs.CV|cs.LG|AI|stat.ML

User: Pass: [Login or Create](#) [Get me on GitHub](#)

Search:

most recent | **top recent** | top type | friends | discussions | recommended | library

Only show v1 | Last day | Last 3 days | **Last week** | Last month | Last year | All time

Top papers based on people's libraries:

Deep Learning: A Critical Appraisal
Gary Marcus
1/2/2018 cs.AI | 97R40 | 1.2.0; 1.2.6
1 figure
[show similar](#) [discuss](#)

DeepMind Control Suite
Yaeli Tassa, Yotam Doron, Alistar Mendel, Tom Erez, Yacine Li, Diego de Las Casas, David Budden, Abbas Abdoalmaleki, Josh Merel, Andrew LeFrancq, Timothy Lillicrap, Martin Riedmiller
1/2/2018 cs.AI
24 pages, 7 figures, 2 tables
[show similar](#) [discuss](#)

deeplearn.org

Deep Learning Monitor
keywords: Add Monitor Recent two weeks

Full-text Search | About | Special Mentions | Hot Papers | Fresh Papers | Hot

Hot Tweets

@OriolMiyaiML
"Optimal" running, brought to you by
Deep RL. <https://arxiv.org/abs/1801.00631>
2018-01-03 [Retweet](#) [Like](#) [Super Hot](#)

@ilyasut
The ML wish of 2018: may all your local minima be global, your variance bounded, your labelled data plentiful, and your compute massive!
2017-12-31 [Retweet](#) [Like](#) [Super Hot](#)

@AndrewWNg
Question for everyone: Can you name a 2017 AI accomplishment (such a technical result, prototype, demo, research paper...)?
<https://twitter.com/AndrewWNg/status/924191910111>
2018-01-02 [Retweet](#) [Like](#) [Super Hot](#)

@khollet
The ML research community has long been driven by the need to publish, which results in a stark, sometimes ridiculous...
<https://twitter.com/khollet/status/924191910111>
2018-01-04 [Retweet](#) [Like](#) [Super Hot](#)

@ylecun
This is to AI as prestidigitation is to real magic. Perhaps we should call this "Cargo Cult AI" or "Potemkin AI" o... <https://twitter.com/ylecun/status/924191910111>
2018-01-04 [Retweet](#) [Like](#) [Super Hot](#)

Hot Papers

DeepMind Control Suite
Yaeli Tassa, Yotam Doron, Alistar Mendel, Tom Erez, Yacine Li, Diego de Las Casas, David Budden, Abbas Abdoalmaleki, Josh Merel, Andrew LeFrancq, Timothy Lillicrap, Martin Riedmiller
2018-01-02 [PDF](#) [Mendeley](#) [Super Hot](#)

Adversarial Patch
Tom B. Brown, Dandelion Mané, Aurko Roy, Martin Abadi, Justin Gilmer
2017-12-27 [PDF](#) [Mendeley](#) [Super Hot](#)

Deep Learning: A Critical Appraisal
Gary Marcus
2018-01-02 [PDF](#) [Mendeley](#) [Super Hot](#)

Recent Advances in Recurrent Neural Networks
Hojjat Salehinejad, Julianne Baarbe, Sharan Senkar, Joseph Barlett, Erol Colak, Shahrokh Valoei
2017-12-28 [PDF](#) [Mendeley](#) [Super Hot](#)

Visualizing the Loss Landscape of Neural Nets
Hao Li, Zheng Xu, Gavin Taylor, Tom Goldstein
2017-12-28 [PDF](#) [Mendeley](#) [Super Hot](#)

CNN is All You Need
Qiming Chen, Chen Xu
2017-12-27 [PDF](#) [Mendeley](#) [Super Hot](#)

Deep learning for universal linear embeddings of nonlinear dynamics
Badrinarayan Jayaram, John M. Brumby, David Rosenberg
2018-01-04 [Retweet](#) [Like](#) [Super Hot](#)

Fresh Papers

Characterizing Adversarial Subspaces Using Local Intrinsic Dimensionality
Xingun Ma, Bo Li, Yaen Wang, Sarah M. Efrani, Sudanthi Wijewickrema, Michael E. Houle, Grant Schoenbeck, Dawn Song, James Bailey
2018-01-08 [PDF](#) [Mendeley](#) [Hot](#)

Spatially transformed adversarial examples
Chaoqun Xiao, Junhan Zhu, Bo Li, Warren He, Mingyue Liu, Dawn Song
2018-01-08 [PDF](#) [Mendeley](#) [Hot](#)

Generating adversarial examples with adversarial networks
Chaoqun Xiao, Bo Li, Junhan Zhu, Warren He, Mingyue Liu, Dawn Song
2018-01-08 [PDF](#) [Mendeley](#) [Hot](#)

LaVAN: Localized and Visible Adversarial Noise
Danny Karmion, Daniel Zoran, Yoav Goldberg
2018-01-08 [PDF](#) [Mendeley](#) [Hot](#)

Unsupervised Discovery of Toxoplasma gondii Motility Phenotypes
Mojib A. Faki, Stephen A. Vella, Silvia H. J. Moreno, Shannon Quinn
2018-01-08 [PDF](#) [Mendeley](#) [Hot](#)

Analyzing Roles of Classifiers and Code-Mixed factors for Sentiment Identification
2018-01-08 [PDF](#) [Mendeley](#) [Hot](#)

reinforce

Applicatio
Reinforce
Biological
Multi-Mahm
Hussain, S
2018-01-04

Soft Actor
Entropy B
Learning
Tomasz Hol
Sergey Lev
2018-01-04

Jointly Le
Control A
Reinforce
Charles Sch
Matthew R
2018-01-04

Unifying F
PAC Boun
Reinforce
Christoph D
Brunskill
2018-01-04

Trading th
Reinforce
Catherine M
2018-01-04

Deep Neu
Algorith

Vienna Deep Learning Meetup



23 April 2018 @ Wien Energie



Ethics & Bias in Artificial Intelligence

May 7th, 2018, 18:30 - 23:00

Precht-Saal, Hauptgebäude, TU Wien

Vienna
Deep
Learning
Meetup



Deep Learning and the Crisis of Trust in Computing

Prof. Moshe Vardi, Rice University

The Big Data Illusion and its Impact on Flourishing with General AI

Prof. Sarah Spiekermann-Hoff, WU Wien

Panel Discussion “Ethics & Bias in AI”

Panelists

Prof. Moshe Vardi

Prof. Peter Purgathofer

Prof. Sarah Spiekermann-Hoff

Prof. Mark Coeckelbergh

Dr. Christof Tschohl

Rice University

TU Wien

WU Wien

Universität Wien

Research Institute Austria

Moderation

Markus Mooslechner

Terra Mater Productions

Event Registration

More information and link for registration: aiethics.cisvienna.com

