Vienna Deep Learning Meetup

23 April 2018 @ Wien Energie

Vienna Deep Learning Meetup

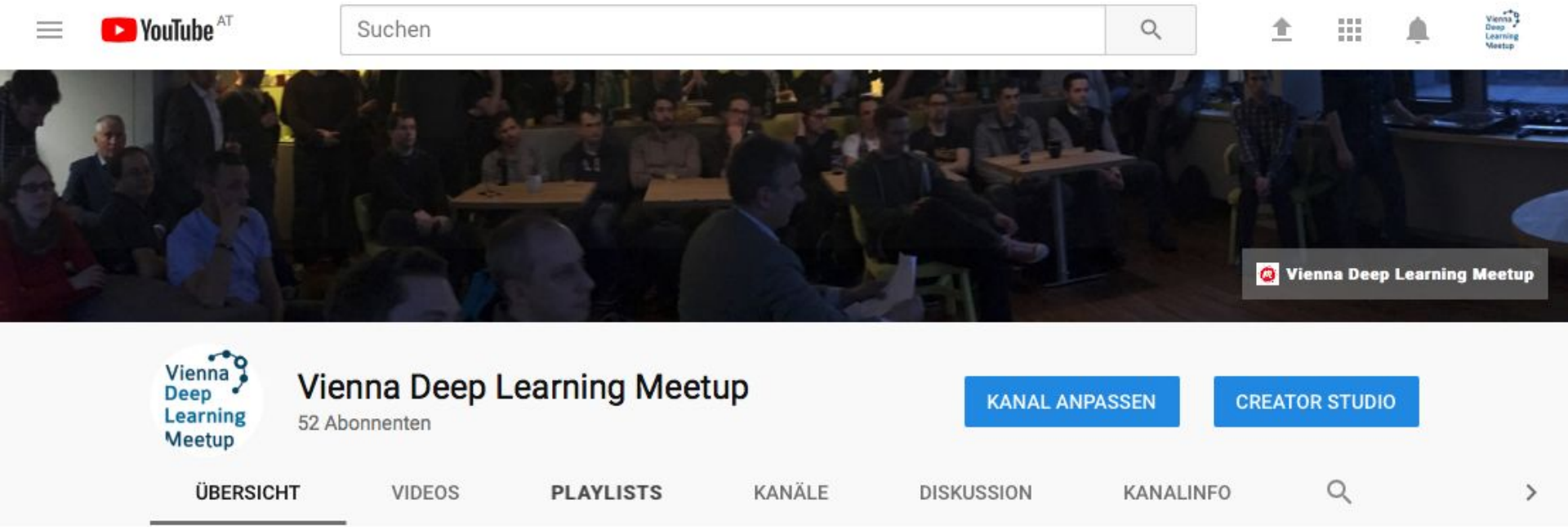
The Organizers:

Thomas Lidy
Musimap

Jan Schlüter
OFAI

Alex Schindler
AIT & TU Wien

New Youtube Channel



LIVE-STREAM tonight!

SUBSCRIBE: http://youtube.com/ViennaDeepLearningMeetup

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

Vienna
Deep Learning
Meetup

SmartStream

WE ARE HIRING

MACHINE LEARNING, DEEP LEARNING, DATA MINING EXPERT

Andreas Burner, SmartStream Innovation Lab

SmartStream

About us …

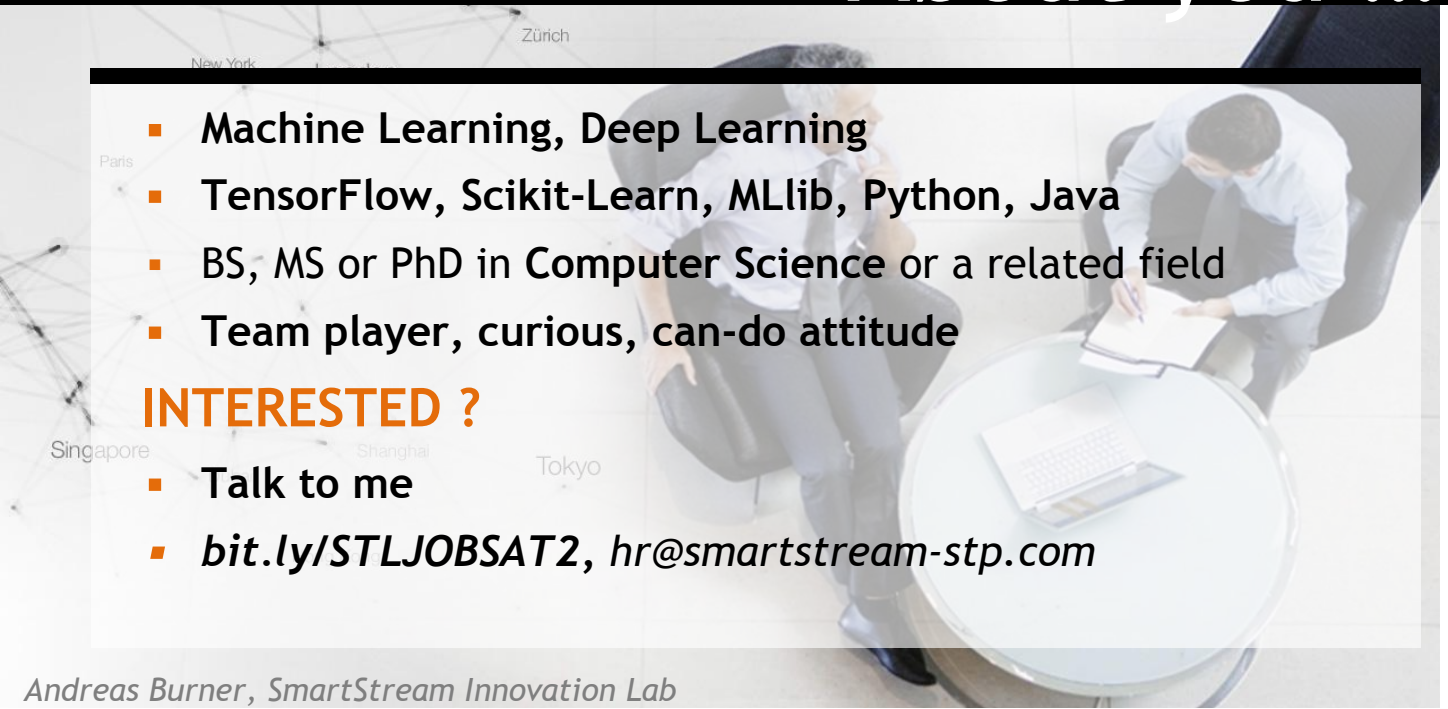
- **Leading software vendor** in the FinTech space
- >**1,500 customers** globally, 70 of the World's top 100 banks

SMARTSTREAM INNOVATION LAB IN VIENNA

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

SmartStream

About you …



- **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

Vienna
Deep Learning
Meetup


CALLING STARTUPS!
Exhibit at the leading trade show
for smart automation and robotics
JOIN US!
19 - 22 JUNE / MUNICH
automatica
MOBILE
WORLD CAPITAL
BARCELONA

Ethics & Bias in Artificial Intelligence

May 7th, 2018, 18:30 - 23:00
Prechtl-Saal, Hauptgebäude, TU Wien

Vienna Deep Learning Meetup

TU WIEN ! CIS

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	Rice University
Prof. Peter Purgathofer	TU Wien
Prof. Sarah Spiekermann-Hoff	WU Wien
Prof. Mark Coeckelbergh	Universität Wien
Dr. Christof Tschohl	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

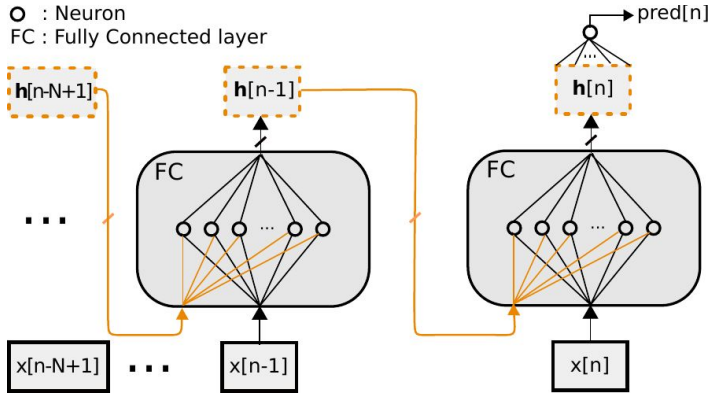
Send us contributions (tom.lidy@gmail.com)
or come with slides to do a short block yourself!

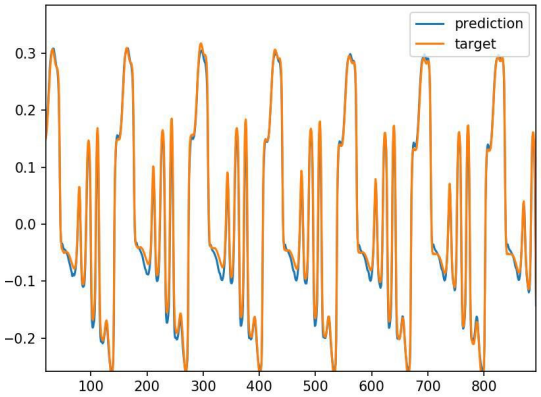
Vienna
Deep Learning
Meetup

Real Time Emulation of Parametric Guitar Tube Amplifier with Long Short Term Memory Neural Network

Thomas Schmitz and Jean-Jacques Embrechts[1]

- 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

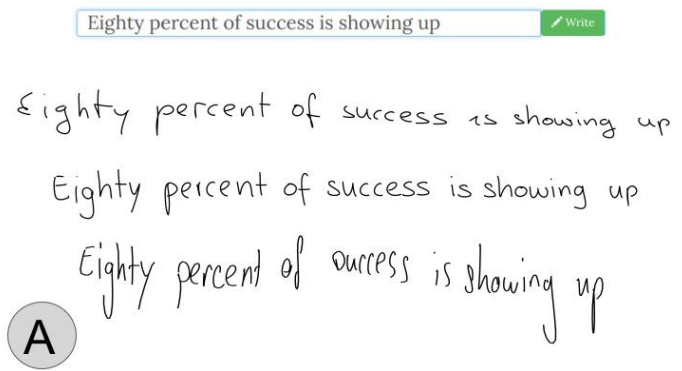


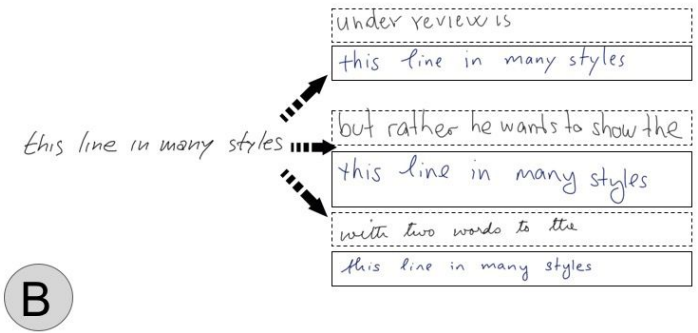


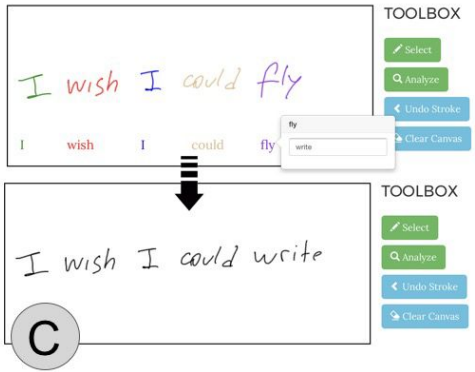
Vienna Deep Learning Meetup

DeepWriting: Making Digital Ink Editable via Deep Generative Modeling

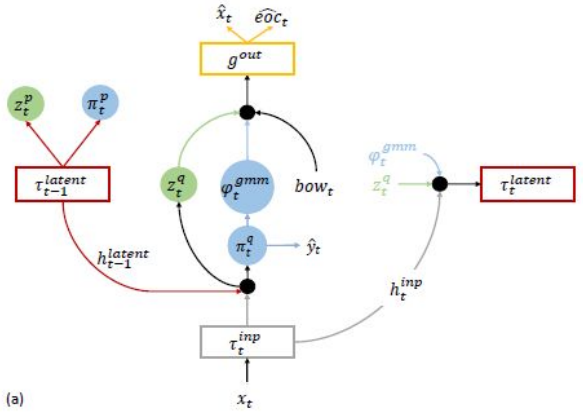
- Handwriting recognition
- Pen-based interaction
- Handwriting Beautification
- Handwriting Synthesis
- Spell-Checking & Correction





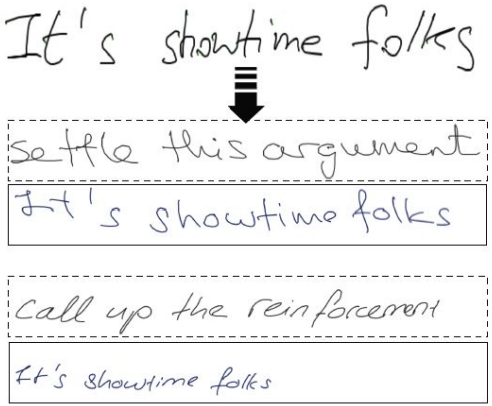


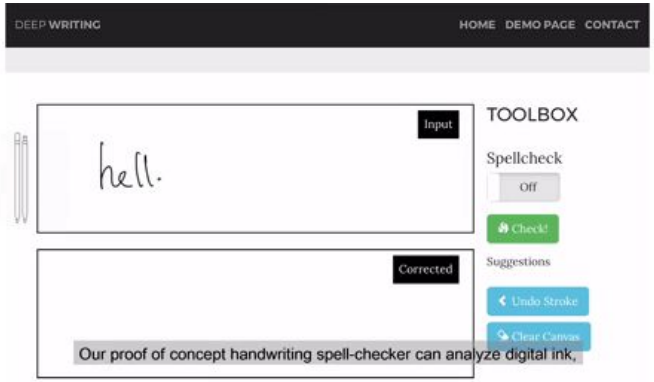
- Conditional Variational Recurrent Neural Network (C-VRNN)
  - introducing a set of latent random variables to
    - increase the expressive power of the model
    - Decouple style from content

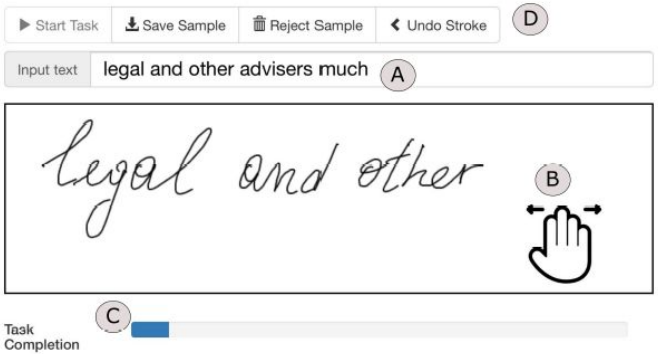


Vienna Deep Learning Meetup

DeepWriting: Examples







Vienna Deep Learning Meetup

Dogs vs. Cats Test

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

Vienna Deep Learning Meetup

Dogs vs. Cats Test

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

Vienna Deep Learning Meetup

Dogs vs. Cats Test

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

Vienna Deep Learning Meetup

Dogs vs. Cats Test

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

Vienna Deep Learning Meetup

Dogs vs. Cats Test

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

Vienna Deep Learning Meetup

Dogs vs. Cats Test

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

Vienna Deep Learning Meetup

Adversarial Examples that Fool both Human and Computer Vision

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

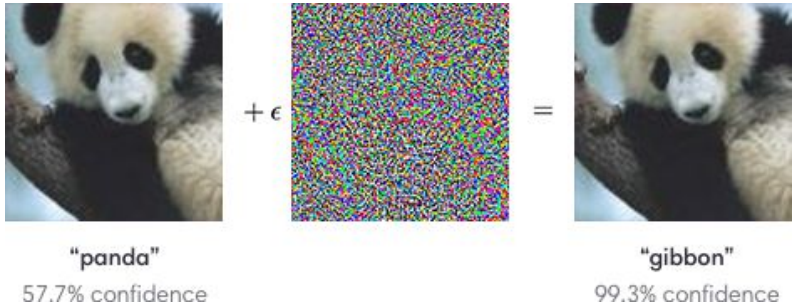
At least at brief exposure, humans are tricked into making the wrong decision as well.

https://arxiv.org/abs/1802.08195

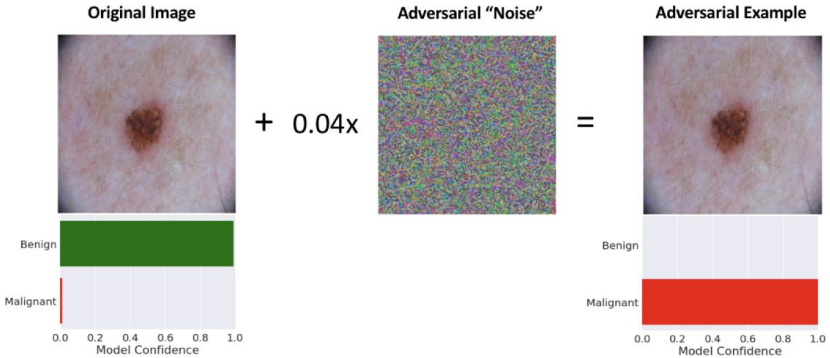
Vienna Deep Learning Meetup

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



https://arxiv.org/abs/1802.08195

https://arxiv.org/abs/1802.08195

Vienna Deep Learning Meetup

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

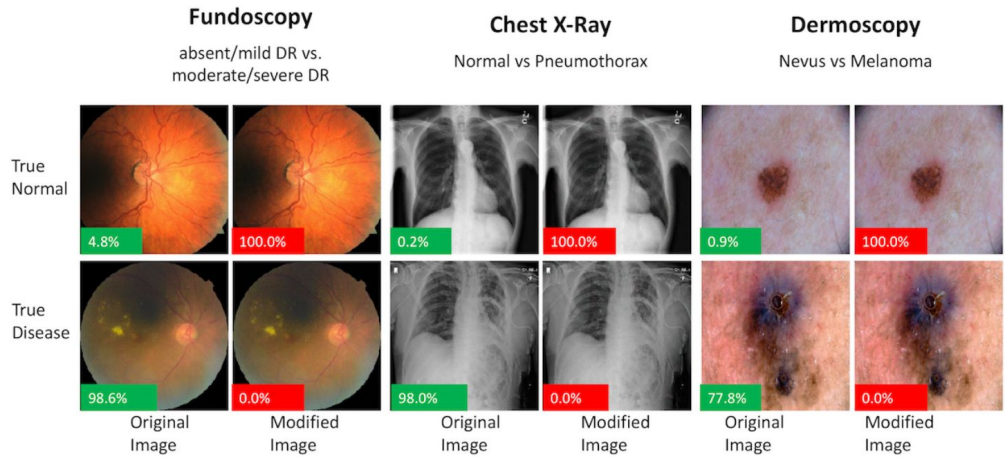
Why is it easy to do that?

- 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

https://arxiv.org/abs/1802.08195

Vienna Deep Learning Meetup

Adversarial Attacks Against Medical Deep Learning Systems



What to do about it?

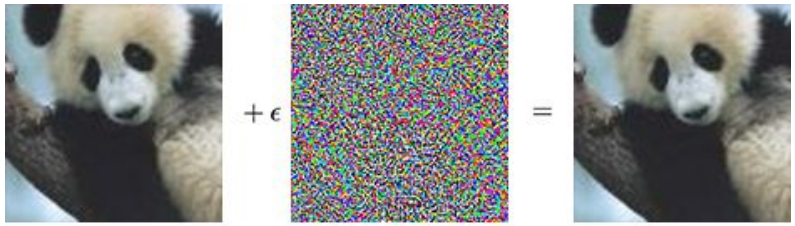
- Algorithmic defenses: ongoing research
- Infrastructural defenses: have imaging devices sign the images to prevent undetected manipulations

https://arxiv.org/abs/1802.08195

Vienna Deep Learning Meetup

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

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



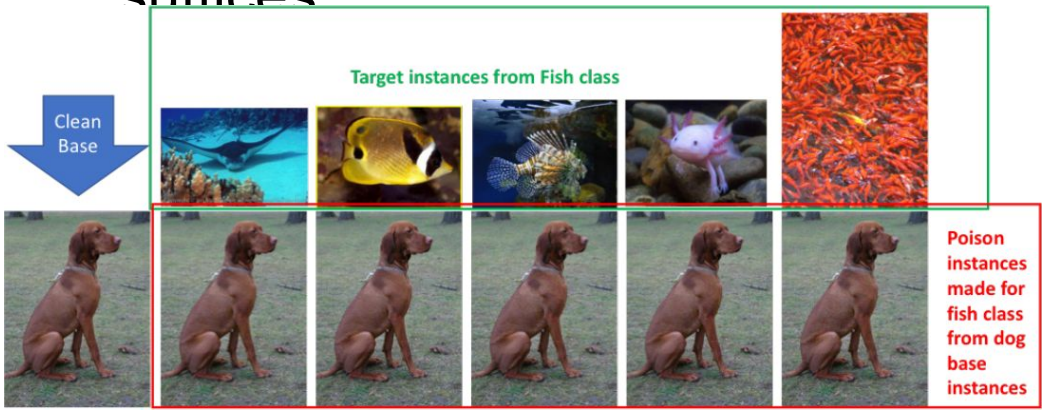
https://arxiv.org/abs/1412.6572

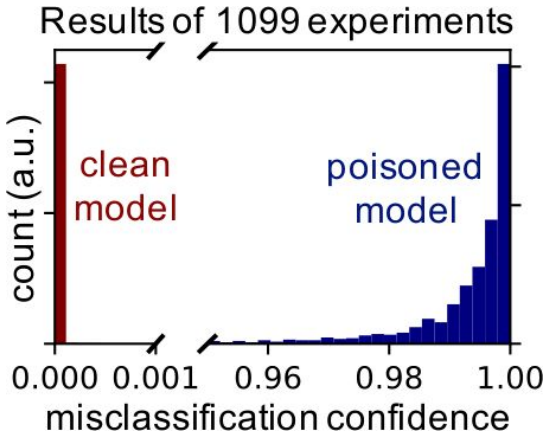
- Adding adversarials to the *training set*, we can manipulate the classification boundary that is learned
- Useful attack vector when we can create training examples for a system that will be labeled by humans

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





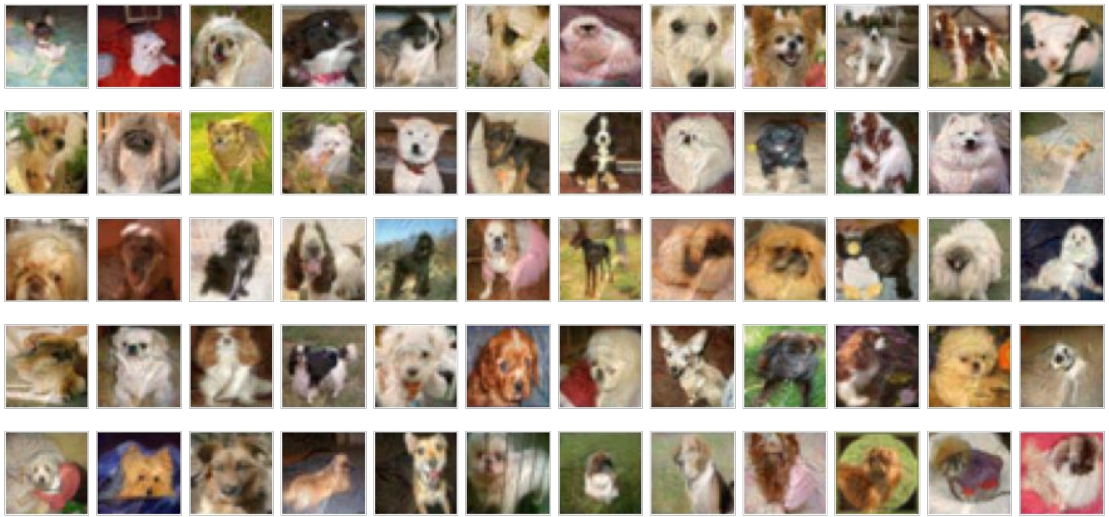
Adding one of the dog images to the training set causes the respective fish image to be misclassified with high confidence.

https://arxiv.org/abs/1804.00792

Vienna Deep Learning Meetup

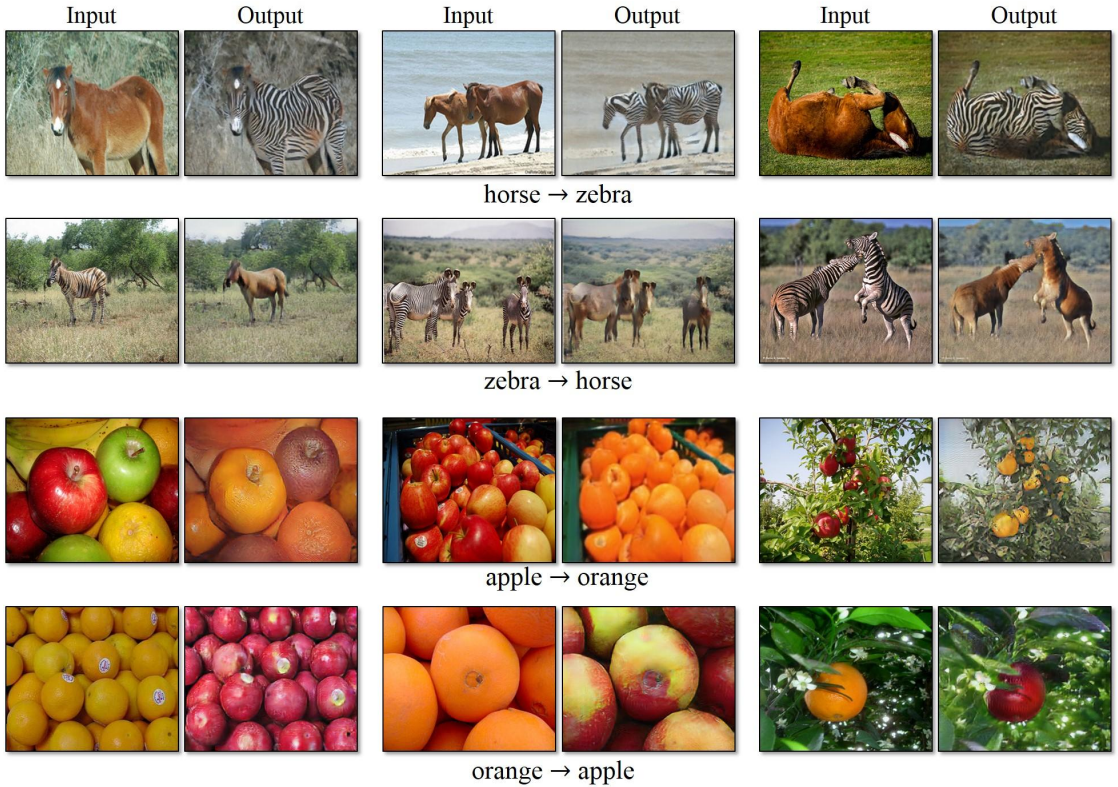
Poison Frogs! Targeted Clean-Label Poisoning Attacks on Neural Networks

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



https://arxiv.org/abs/1804.00792

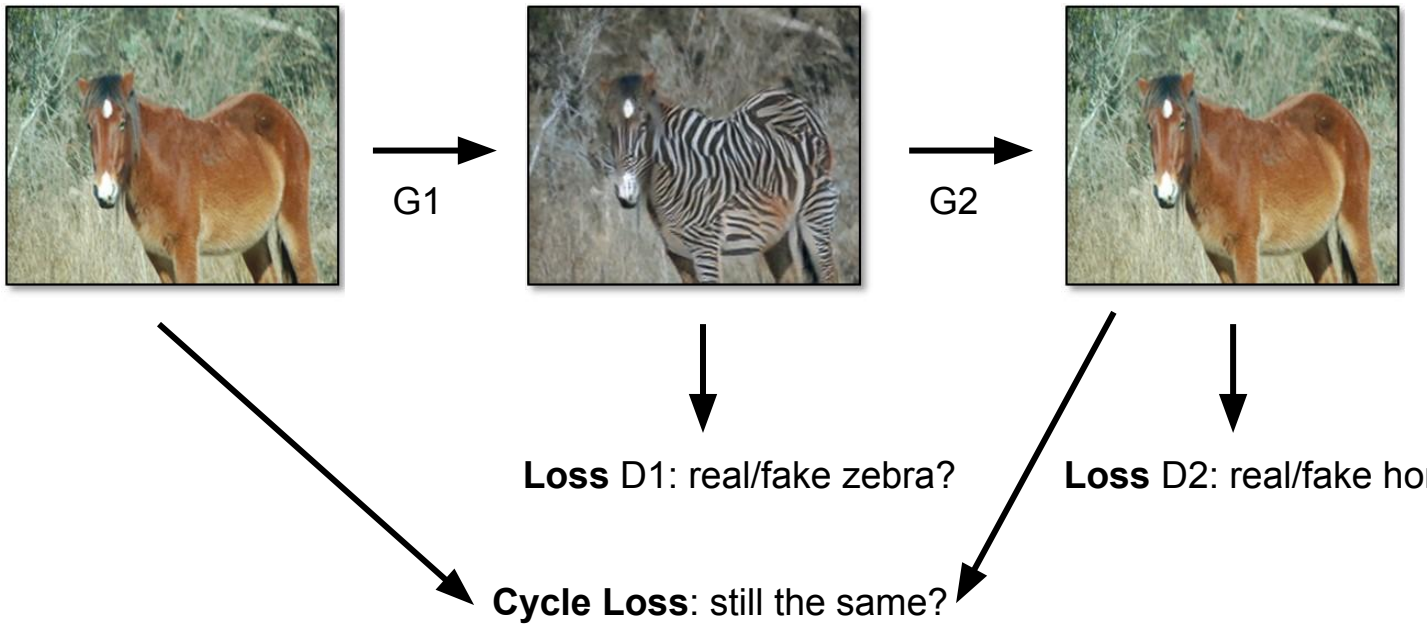
CycleGAN, a Master of Steganography



https://arxiv.org/abs/1712.02950

Vienna Deep Learning Meetup

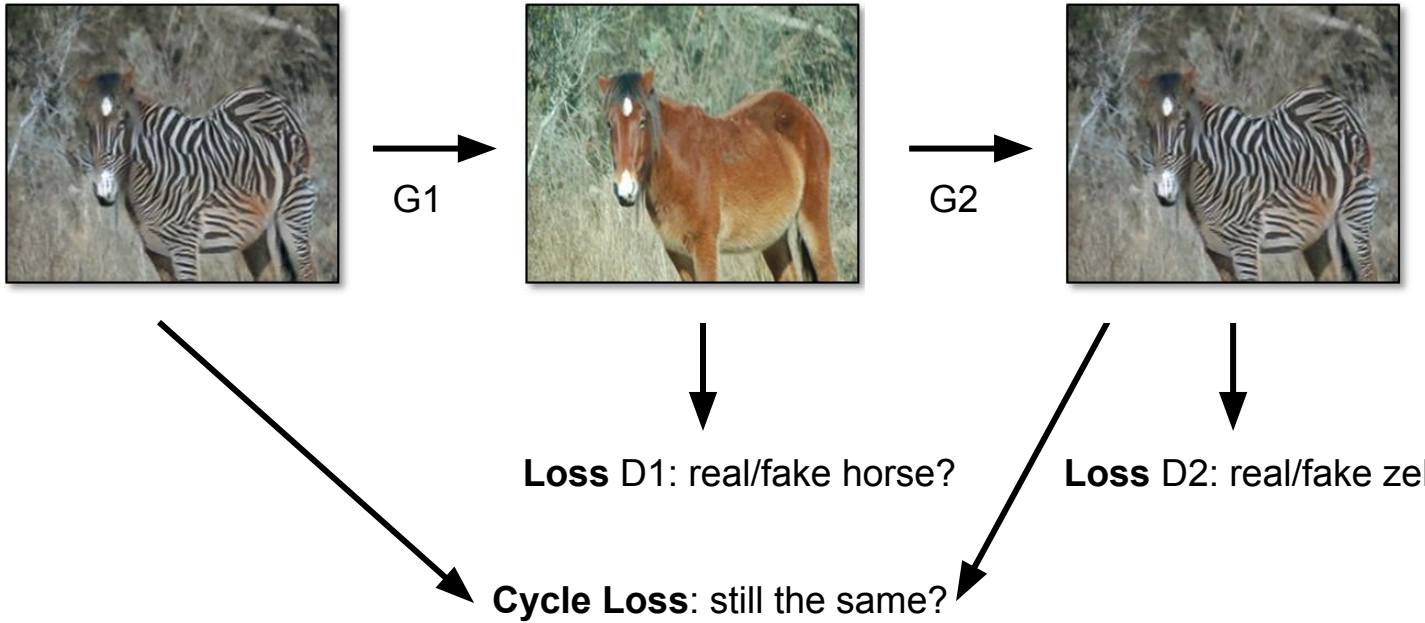
CycleGAN, a Master of Steganography



https://arxiv.org/abs/1712.02950

Vienna Deep Learning Meetup

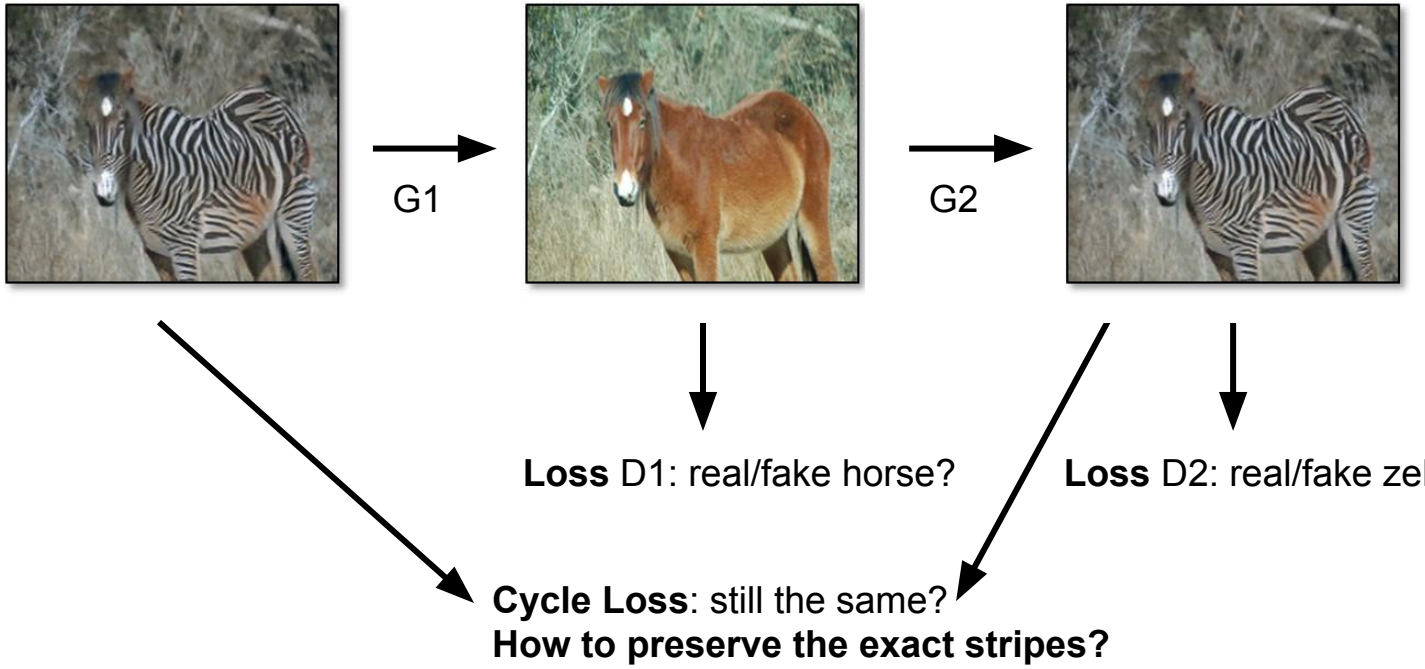
CycleGAN, a Master of Steganography



https://arxiv.org/abs/1712.02950

Vienna Deep Learning Meetup

CycleGAN, a Master of Steganography



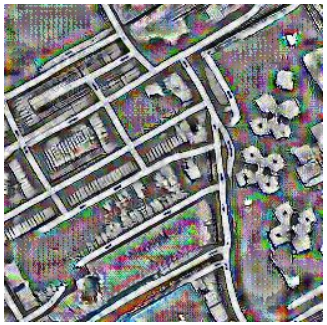
https://arxiv.org/abs/1712.02950

Vienna Deep Learning Meetup

CycleGAN, a Master of Steganography

G1

G2



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

https://arxiv.org/abs/1712.02950

Vienna Deep Learning Meetup

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

https://arxiv.org/abs/1804.04806

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}
}}
```

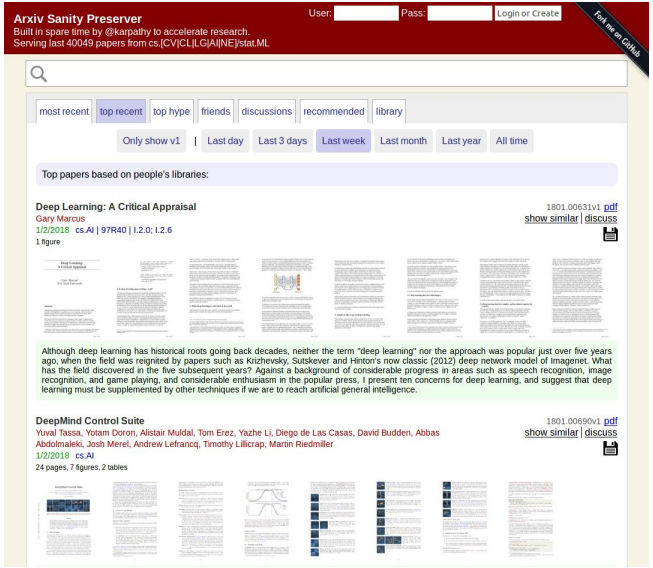

Tensor Comprehension for 2D Average Pooling

https://arxiv.org/abs/1802.04730

Vienna Deep Learning Meetup

Tons more

arxiv-sanity.com



deeplearn.org

Vienna Deep Learning Meetup

Vienna Deep Learning Meetup

23 April 2018 @ Wien Energie

Ethics & Bias in Artificial Intelligence

May 7th, 2018, 18:30 - 23:00
Prechtl-Saal, Hauptgebäude, TU Wien

Vienna Deep Learning Meetup

TU WIEN ! CIS

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	Rice University
Prof. Peter Purgathofer	TU Wien
Prof. Sarah Spiekermann-Hoff	WU Wien
Prof. Mark Coeckelbergh	Universität Wien
Dr. Christof Tschohl	Research Institute Austria

Moderation

Markus Mooslechner	Terra Mater Productions

Event Registration
More information and link for registration: **aiethics.cisvienna.com**