DeepLearn School - Guimaraes

Matthieu François - Simon Lebeaud - Nicolas Tirel

GreenAI U.P.P.A.

May 2, 2022

Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

2 Graph Lecture

- **3** Biometrics Trustworthiness
- 4 Medicine, high physics and Weather
- **5** Ecology survey

Matthieu François - Simon Lebeaud - Nicolas Tirel

Figures Structure

2 Graph Lecture

Biometrics Trustworthiness

4 Medicine, high physics and Weather

5 Ecology survey



2 Graph Lecture

Biometrics Trustworthiness

④ Medicine, high physics and Weather

6 Ecology survey

- 《日》 《聞》 《臣》 《臣》 『臣』 ろんの

Matthieu François - Simon Lebeaud - Nicolas Tirel

3 keynotes

Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

- 3 keynotes
- 21 lectures

/latthieu François - Simon Lebeaud - Nicolas Tirel

- 3 keynotes
- 21 lectures 3*1h30 lecture each
 - Interpretability
 - Generative Models
 - Vision
 - Audio
 - .

- 3 keynotes
- 21 lectures 3*1h30 lecture each
 - Interpretability
 - Generative Models
 - Vision
 - Audio
 - .
- 160 participants



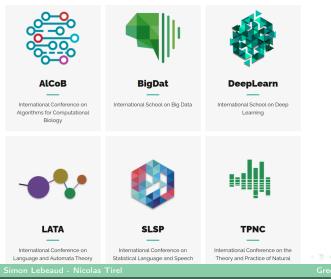
- 2 Graph Lecture
- Biometrics Trustworthiness
- 4 Medicine, high physics and Weather
- **6** Ecology survey

- <ロ> (四> <回> <回> (日>)

Matthieu François - Simon Lebeaud - Nicolas Tirel

Structure

Institute for Research Development, Training and Advice



② Graph Lecture

Presentation Applications fields Graph types Some Methods Graph Embedding DeepLearning based embedding

Biometrics Trustworthiness

4 Medicine, high physics and Weather

6 Ecology survey

② Graph Lecture

Presentation

Applications fields Graph types Some Methods Graph Embedding DeepLearning based embedding

Biometrics Trustworthiness

4 Medicine, high physics and Weather

5 Ecology survey

Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

Presentation

Lecturer: Michalis Vazirgiannis Theme: Graph Mining - generators & community detection

Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

2 Graph Lecture

Presentation

Applications fields

Graph types Some Methods Graph Embedding DeepLearning based embedding

Biometrics Trustworthiness

4 Medicine, high physics and Weather

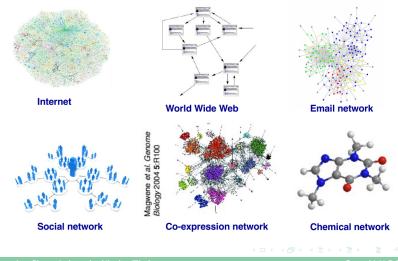
6 Ecology survey

Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

Applications fields



Matthieu François - Simon Lebeaud - Nicolas Tirel

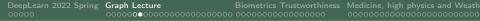
② Graph Lecture

Presentation Applications fields **Graph types** Some Methods Graph Embedding DeepLearning based embeddin

Biometrics Trustworthiness

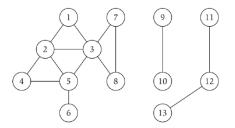
4 Medicine, high physics and Weather

6 Ecology survey



Graph types

Overview of graph types : directed, unidirected, complete, tree, bipartite graphs...



Isomorphism = best similarity between 2 graphs

2 Graph Lecture

Presentation Applications fields Graph types Some Methods

Graph Embedding DeepLearning based embedding

Biometrics Trustworthiness

4 Medicine, high physics and Weather

6 Ecology survey

Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

Graph Generation

Aim: simulate graph data with same distribution / patern

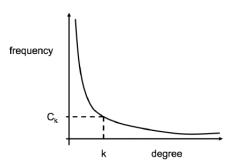
• Regarding dregree law

Aatthieu François - Simon Lebeaud - Nicolas Tirel

Graph Generation

Aim: simulate graph data with same distribution / patern

• Regarding dregree law

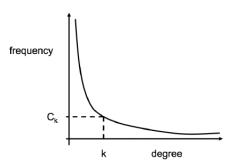


We visualise number of neighbors for each node in graph

Graph Generation

Aim: simulate graph data with same distribution / patern

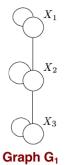
Regarding dregree law



We visualise number of neighbors for each node in graph

Regarding subpatern (Kronecker model)

Graph Lecture



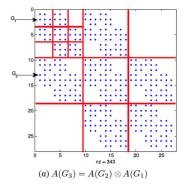
 $X_{1,3}$ $X_{1,1}$ $X_{2,3}$ $X_{2,1}$ $X_{2,2}$ $X_{3,1}$ $X_{3,2}$ $X_{3,3}$

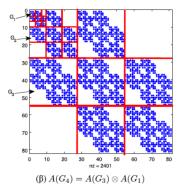
 $X_{1,2}$

 $X_{1,1}$

Graph $G_2 = G_1 \boxtimes$ G₁

Graph Generation





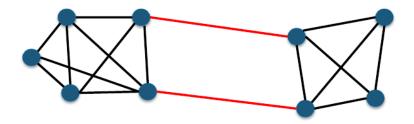
Matthieu François - Simon Lebeaud - Nicolas Tire

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

Clustering

- based on number of triangles
- based on number of edges



シック・ 川 ・ ・ 川川・ ・ 一門・ ・ 白 ・

Matthieu François - Simon Lebeaud - Nicolas Tirel

GreenAI U.P.P.A.

Clustering

- based on modularity (Louvain, Newman-Girvan)
- based on deeplearning (auto-encoder & node embedding)

② Graph Lecture

Presentation Applications fields Graph types Some Methods

Graph Embedding

DeepLearning based embedding

Biometrics Trustworthiness

4 Medicine, high physics and Weather

6 Ecology survey

Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

Embedding & Similarity study

Aim

Create Embedding vectors for nodes, keeping proximity and similarity edges between them.

Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

Embedding & Similarity study

Aim

Create Embedding vectors for nodes, keeping proximity and similarity edges between them.

How to?

We could take the adjacency matrix as embedding but inner product between them would produce a lot of 0.

$$\begin{pmatrix} 0 & 1 & \dots & 0 \\ 1 & 0 & \dots & 1 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 1 & \dots & 0 \end{pmatrix}$$

Embedding & Similarity study

Many methods:

based on kernel

Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

Embedding & Similarity study

Many methods:

 based on kernel Better than DeepLearning Methods but not scalable on big data.

Embedding & Similarity study

Many methods:

- based on kernel Better than DeepLearning Methods but not scalable on big data.
- based on deep learning

2 Graph Lecture

Presentation Applications fields Graph types Some Methods Graph Embedding DeepLearning based embedding

Biometrics Trustworthiness

4 Medicine, high physics and Weather

6 Ecology survey

Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

Laplacian eigenmaps

Early Method: matrix-factorization using Laplacian eigenmaps

Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

Laplacian eigenmaps

Early Method: matrix-factorization using Laplacian eigenmaps

• Laplacian eigenmaps projects two nodes i and j close to each other when the weight of the edge between the two nodes A_{ij} is high

Laplacian eigenmaps

Early Method: matrix-factorization using Laplacian eigenmaps

• Laplacian eigenmaps projects two nodes i and j close to each other when the weight of the edge between the two nodes A_{ij} is high

$$y^* = argmin \sum (y_i - y_j)^2 A_{ij} \tag{1}$$

With $A_i j$ the edge weight between i and j.

DeepWalk

Recent Method: inspired by Language Modeling DeepWalk

Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

DeepWalk

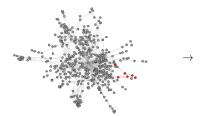
Recent Method: inspired by Language Modeling DeepWalk

• Employ random walks to capture structural relationships between nodes. Each sample can be considered as a "sentence" of a document in NLP.

DeepWalk

Recent Method: inspired by Language Modeling DeepWalk

 Employ random walks to capture structural relationships between nodes. Each sample can be considered as a "sentence" of a document in NLP.



$$\begin{split} & v_5 \rightarrow v_8 \rightarrow v_{32} \rightarrow v_{28} \rightarrow v_6 \rightarrow v_{10} \rightarrow v_9 \\ & v_3 \rightarrow v_5 \rightarrow v_{28} \rightarrow v_8 \rightarrow v_9 \rightarrow v_{10} \rightarrow v_{25} \\ & v_{20} \rightarrow v_{10} \rightarrow v_{12} \rightarrow v_6 \rightarrow v_8 \rightarrow v_4 \rightarrow v_5 \\ & v_{23} \rightarrow v_5 \rightarrow v_{32} \rightarrow v_{10} \rightarrow v_8 \rightarrow v_3 \rightarrow v_1 \\ & v_4 \rightarrow v_3 \rightarrow v_1 \rightarrow v_5 \rightarrow v_1 \rightarrow v_{12} \rightarrow v_{10} \end{split}$$

Aatthieu François - Simon Lebeaud - Nicolas Tirel

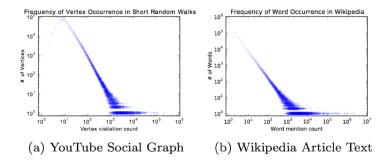
DeepLearn School - Guimaraes

GreenAI U.P.P.A.

26 / 80

Why Random Walk?

Why Random Walk?



RandomWalk nodes distribution is the same as words in Wikipedia article.

DeepWalk

Next step: Use skipgram to generate embedding

• two sampling strategies, to capture:

Aatthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

28 / 80

DeepWalk

Next step: Use skipgram to generate embedding

- two sampling strategies, to capture:
 - structure: depth-first sampling (DFS)
 - local similarity: breadth-first sampling (BFS)

Vlatthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

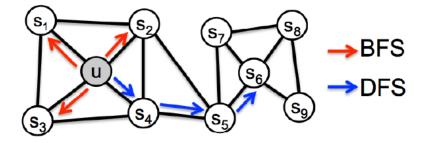
GreenAI U.P.P.A.

28 / 80

DeepWalk

Next step: Use skipgram to generate embedding

- two sampling strategies, to capture:
 - structure: depth-first sampling (DFS)
 - local similarity: breadth-first sampling (BFS)

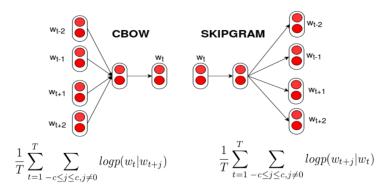


Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

DeepWalk



Matthieu François - Simon Lebeaud - Nicolas Tire

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

Other Methods

It exists also

- GraRep
- Line
- SDNE

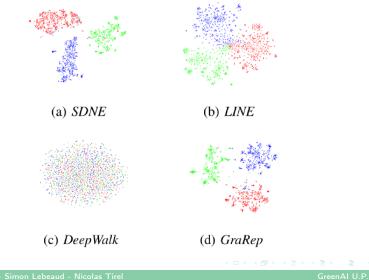
Vlatthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

30 / 80

Other Methods



Matthieu François - Simon Lebeaud - Nicolas Tire

DeepLearn 2022 Spring

Oraph Lecture

Biometrics Trustworthiness Countering Physical Attacks Countering Digital Attacks

4 Medicine, high physics and Weather

5 Ecology survey

Matthieu François - Simon Lebeaud - Nicolas Tirel

Challenges

 Proofing face recognition for security control (public security, border control, building access, face purchase...)



▲口▼▲雪▼▲雪▼▲雪▼ 雪 めんの

Matthieu François - Simon Lebeaud - Nicolas Tirel

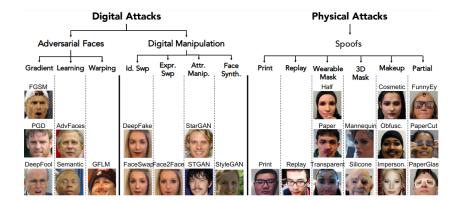
Challenges

- Proofing face recognition for security control (public security, border control, building access, face purchase...)
- Remove ubiquitous presence of deepfake and preventing rapid dissemination of "fake news"



Matthieu François - Simon Lebeaud - Nicolas Tire

Attack types



Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

DeepLearn 2022 Spring

Oraph Lecture

Biometrics Trustworthiness Countering Physical Attacks Countering Digital Attacks

4 Medicine, high physics and Weather

6 Ecology survey

Matthieu François - Simon Lebeaud - Nicolas Tirel

Anti Physical Spoofing Methods

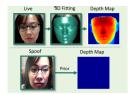


Figure 1: Depth Estimation

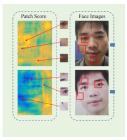
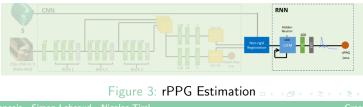


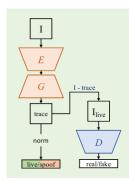
Figure 2: Patch-based CNNs



viattnieu François - Simon Lebeaud - Nicolas

Generative FAS

- CNN is trained to generate a spoof trace image
- Spoof is considered as an added layer to your original image
- If we can generate the spoof layer from a false image then we are capable of taking it of the image and then "recover" the original image



DeepLearn 2022 Spring

Oraph Lecture

- Biometrics Trustworthiness Countering Physical Attacks Countering Digital Attacks
- 4 Medicine, high physics and Weather

5 Ecology survey

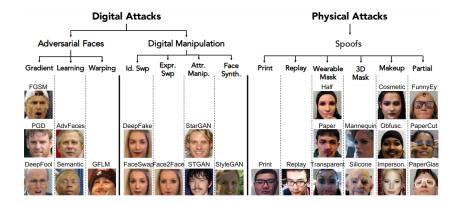
Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

38 / 80

Attacks



Matthieu François - Simon Lebeaud - <u>Nicolas Tire</u>

Dynamic Methods -> Inconsistent Head Poses

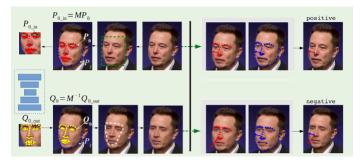


Figure 4: Xin et al. Exposing deep fakes using inconsistent head poses

Matthieu François - Simon Lebeaud - Nicolas Tirel

Static Methods -> Face X-Ray

Detect images altered by the blending of a new face on the original



Figure 5: Li et al. Face X-ray for more general face forgery detection

Matthieu François - Simon Lebeaud - Nicolas Tirel

Multi manipulation detection

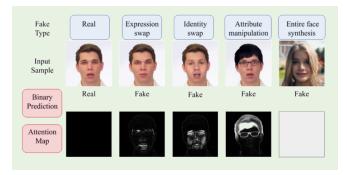


Figure 6: Dang et al. On the Detection of Digital Face Manipulation

Matthieu François - Simon Lebeaud - Nicolas Tirel

Multi manipulation detection

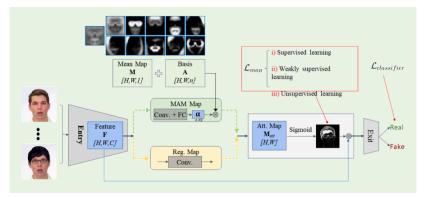


Figure 7: Dang et al. On the Detection of Digital Face Manipulation

Matthieu François - Simon Lebeaud - Nicolas Tirel

Proactive schemes

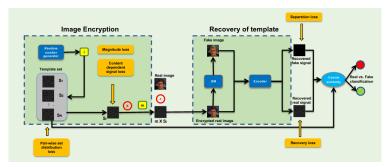


Figure 8: Framework to proactively counter digital spoofing

Matthieu François - Simon Lebeaud - Nicolas Tirel

Adversarial Attacks

- Obfuscation attack: Falsely reject a genuine subject
- Impersonation attack: falsely match to an impostor subject

Solutions:

- Detection
- Purification
- Robustness

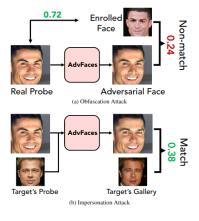


Figure 9: AdvFaces: Adversarial Face Synthesis

Matthieu François - Simon Lebeaud - Nicolas Tirel

Unified Detection of Digital and Physical Face Attacks

- Cluster each types of attacks with high similarities to form groups
- Train a multi-branch model each branch trying to do classification for a cluster of attacks
- Fuse the classification for each cluster

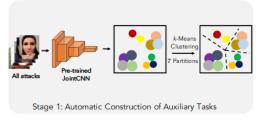


Figure 10: JointCNN: 53.19% TDR

Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

46 / 80

Proposed UniFAD

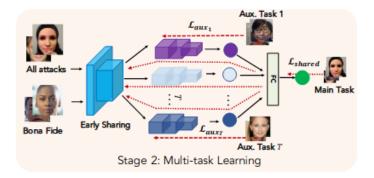


Figure 11: Debayan Deb, Xiaoming Liu, Anil Jain, Unified Detection of Digital and Physical Face Attacks

Matthieu François - Simon Lebeaud - Nicolas Tirel

UniFAD Results

TDR (%) @ 0.2% FDR		Year	Proposed For	Adv.	Dig. Man.	Phys.	Overall	Time (ms)
w/o Re-train	FaceGuard	2020	Adversarial	99.91	22.28	00.58	29.64	01.41
	FFD	2020	Digital Manipulation	09.49	94.57	01.25	34.55	11.57
	SSRFCN	2020	Spoofs	00.25	00.76	93.19	22.71	02.22
	MixNet	2020	Spoofs	00.36	09.83	78.21	21.12	12.47
Baselines	FaceGuard	2020	Adversarial	99.86	41.56	04.35	56.69	01.41
	FFD	2020	Digital Manipulation	76.06	91.32	87.43	68.25	11.57
	SSRFCN	2020	Spoofs	08.23	27.67	89.19	43.26	02.22
	One-class	2020	Spoofs	04.81	45.96	79.32	39.40	07.92
	MixNet-UniFAD	2021	All	82.33	91.59	94.60	90.07	12.47
Fusion Schemes	Cascade	_	-	88.39	81.98	69.19	77.46	05.16
	Min-score	_	-	03.65	11.08	00.43	07.22	16.14
	Median-score	_	-	10.87	42.33	47.19	39.48	16.12
	Mean-score	_	_	14.53	47.18	61.32	38.23	16.12
	Max-score	_	-	85.32	61.93	56.87	73.89	16.13
	Sum-score	-	-	74.93	58.01	50.34	69.21	16.11
	LightGBM	_	-	76.25	81.28	88.52	85.97	17.92
	Proposed UniFAD	2021	All	92.56	97.21	98.76	94.73	02.59

Figure 12: Debayan Deb, Xiaoming Liu, Anil Jain, Unified Detection of Digital and Physical Face Attacks

Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn 2022 Spring

2 Graph Lecture

Biometrics Trustworthiness

4 Medicine, high physics and Weather

Sofia Vallecorsa- Generative Models in High Energy Physics: Examples from CERN

Lucila Ohno-machado - Use of Predictive Models in Medicine and Biomedical Research

Rylan Conway - Deep Learning for Digital Assistants Martin Schultz - Deep Learning for Air Quality, Weather and Climate

DeepLearn 2022 Spring

2 Graph Lecture

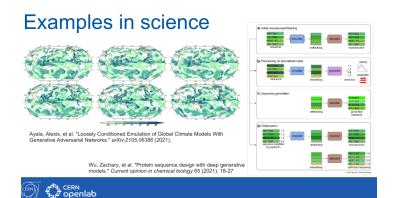
Biometrics Trustworthiness

4 Medicine, high physics and Weather Sofia Vallecorsa- Generative Models in High Energy Physics: Examples from CERN

Lucila Ohno-machado - Use of Predictive Models in Medicine and Biomedical Research

Rylan Conway - Deep Learning for Digital Assistants Martin Schultz - Deep Learning for Air Quality, Weather and Climate

Generative models



Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

Replace with DNN

Accelerating the training process

- Introducing techniques to parallelise training
- Data parallelism
 - Compute gradients on several batches independently
 - Update the model synchronously or asynchronously
- Model Parallelism, Hybrid techniques
- Use reduced precision representation (INT6, BF16, ...)
- Extreme parallelism using combined strategies and SGD algorithm optimisation
 - DeepSpeed and ZeRO-2 on Microsoft Azure





https://www.microsoft.com/enus/research/blog/deepspeed-extreme-scale-modeltraining-for-everyone/



tthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAl U.P.P.A.

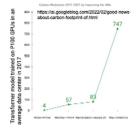
52 / 80

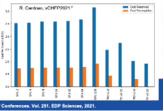
Sustainable AI

Sustainable Al

- Al inference more energy efficient than classical algorithms
- · Energy cost of Al training can be high
- The community is defining best practices¹
 - Efficient Al architectures can reduce computation by 3x– 10x.
 - Al-optimized processors vs general-purpose can improve energy efficiency by 2x-5x².
 - Cloud computing vs on-prem reduces energy usage by 1.4x-2x
- Efficient training strategies
 - · Self-supervision, few-short learning, pre-training



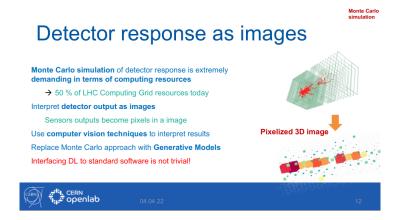




・ 4 回 ト 4 三 ト 4 三 ト 9 4 (*)

Matthieu François - Simon Lebeaud - Nicolas Tirel

Detector Response



Matthieu François - Simon Lebeaud - Nicolas Tirel



The first model: CaloGAN

Learning Particle Physics by Example: Location-Aware Generative Adversarial Networks for Physics Synthesis

CALOGAN: Simulating 3D High Energy Particle Showers in Multi-Layer Electromagnetic Calorimeters with Generative Adversarial Networks

Michela Paganini,^{1,2,*} Luke de Oliveira,^{2,†} and Benjamin Nachman^{2,1} ¹Department of Physics, Yale University, New Haven, CT 06520, USA ²Lourence Berbeley National Laboratory, Berkieg, CA, 94720, USA (Disci: Jamary 1, 2018)

The proton moduling of substantics particle interactions and propagation through nature is the proton moduling of substantics particle interactions and propagation through nature is the proton moduling of the proton of the proton particle of the proton particle of the proton particle interaction of the lower labels (CME): 116 of stated modeling, of the full comparison of priority presents the proton particle of the proton particle particle of the proton particle of the proton particle of the proton particle of the proton particle particle of the particle particle of the particle particle of the particle particle particle of the particle of the particle particle of the particle particle of the particle of the particle particle of the particle particle of the particle particle particle of the particle p

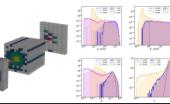
Luke de Oliveira", Michela Paganini"³, and Benjamin Nachman"

^aLeverace Berkeley National Laboratory, J Cycletran R4, Berkeley, CA, MYD0, USA ^bDepartment of Physics, Yale University, New Euror, CT 46530, USA

E-muil: lukedeeliveira01b1.gov, michela.paganini0yale.edu, bmachnam0owrn.ch

Ameraces: We provide a bodge browse generative modeling in the Modine Lorating commutes an similarity dipode processon in light. Emerge provide Propts by paying a new Generative Advanced Review, (EGAN) estimations to the production of pit mapse - 2D responsibilities of the Communication of the Communication of the Communication of the Loratice Asset: Generations Modernian Horsen, balances and the Communication of the Loratice Asset: Generations Modernian Horsen, balances and the Communication of the Loratice Asset: Generations Modernian Horsen (GAN) essential balances proteom communications Modernian Horsen (Horsen et al. 1996). The Loratice Asset: Generation Longent and the Complex Asset: Marken and Modernian Horsen (Horsen et al. 1996). The Loratice Asset: Generation Longent and the Communication of CoMA is on an other simulation in Balance (Horsen et al. 1996). The Loratice Asset: Generation and the Loratice Asset: Generation Horsen (Horsen et al. 1996). The Loratice Asset: Generation Horsen et al. 1996 (Horsen et al. 1996). The Loratice Asset: Generation Horsen et al. 1996 (Horsen et al. 1996). The Loratice Asset: Generation Horsen et al. 1996 (Horsen et al. 1996). The Loratice Asset: Generative Horsen et al. 1996 (Horsen et al. 1996). The Loratice Asset: Generative Horsen et al. 1996 (Horsen et al. 1996). The Loratice Asset: Generative Horsen et al. 1996 (Horsen et al. 1996). The Loratice Asset: Generative Horsen et al. 1996 (Horsen et al. 1996). The Loratice Asset: Generative Horsen et al. 1996 (Horsen et al. 1996). The Loratice Asset: Generative Horsen et al. 1996 (Horsen et al. 1996). The Loratice Asset: Generative Horsen et al. 1996 (Horsen et al. 1996). The Loratice Asset: Generative Asset: Generat





メロト (個) (言) (言) (言) ほうのの()

Matthieu François - Simon Lebeaud - Nicolas Tire

DeepLearn 2022 Spring

2 Graph Lecture

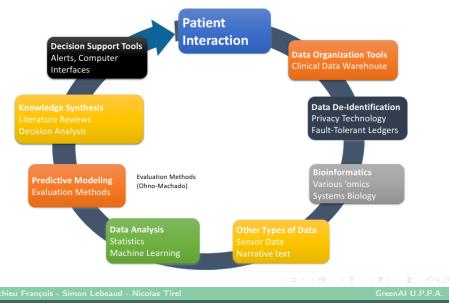
Biometrics Trustworthiness

Medicine, high physics and Weather Sofia Vallecorsa- Generative Models in High Energy Physics: Examples from CERN Lucila Ohno-machado - Use of Predictive Models in Medicine

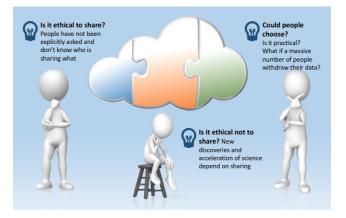
and Biomedical Research

Rylan Conway - Deep Learning for Digital Assistants Martin Schultz - Deep Learning for Air Quality, Weather and Climate

Introduction



Data sharing



Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

Data sharing

Privacy vs. Data Sharing

- · Personalized medicine depends on big data
- Getting enough data to study rare diseases is already difficult without thinking of privacy risks
- It is difficult to quantify the privacy risk and potential benefits
- Streamlined access-controlled sharing: quickly determine who will use the data and why, and provide controlled access
 - Authenticate Users & Authorize Users
 - Monitor Use



Source: DOE

GreenAl

Matthieu François - Simon Lebeaud - Nicolas Tire

De-identification

People think *re-identification* means finding the names (of everyone) in the database

	biometric		diagnosis	income
Lisa	ABDSFHG		pregnancy	60k
Mike	BQEHGKK		rare disease 1	100k
Alice	WOEIMIV		depression	20k
	Α	в	diagnosis	income
	~		ulughosis	meonie
Lico	40	20		601
Lisa	10	20	pregnancy	60k
Lisa Mike	10 10	20 21	pregnancy rare disease 1	60k 100k

Matthieu François - Simon Lebeaud - Nicolas Tirel

Re-identification

But they forget someone can target an individual								
	biometric		diagnosis	income				
	ABDSFHG		pregnancy	60k				
l know something	BQEHGKK		rare disease 1	100k				
	WOEIMIV		depression	20k				
	Α	в	diagnosis	income	But I want to			
about the	10	20	pregnancy	60k	know more			
target person	10	21	rare disease 1	100k				
	11	20	depression	20k				
	Α	в	diagnosis	income				
	10	20	pregnancy	60k				
	10	21	rare disease 1	100k				
	11	20	depression	20k	k anonymity,			
	10	20	pregnancy	20k	l-diversity,			

Matthieu François - Simon Lebeaud - <u>Nicolas Tirel</u>

DeepLearn 2022 Spring

2 Graph Lecture

Biometrics Trustworthiness

Medicine, high physics and Weather Sofia Vallecorsa- Generative Models in High Energy Physics: Examples from CERN Lucila Ohno-machado - Use of Predictive Models in Medicine and Biomedical Research Rylan Conway - Deep Learning for Digital Assistants Martin Schultz - Deep Learning for Air Quality, Weather and Climate

Full ASR

ASR System Overview

This task is commonly approached by breaking it down into subproblems

- · Wake Word Detection: identifying when the user is speaking to the assistant
- Acoustic modeling: transforming the raw audio signal into units of spoken language called "phonemes" (these usually map directly to sub-word tokens)
- Pronunciation modeling: mapping sequences of phonemes into words
- · Language modeling: assign probabilities to word sequences
- Decoding: determine which word sequence is most likely to represent to the input audio signal

Key word selection

Wake Word Detection

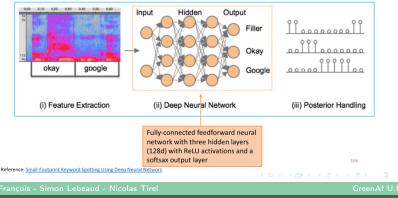
- The first step in the ASR pipeline for digital assistants is Wake Word Detection
 - This is a special case of Keyword Spotting (KWS), a larger subfield of ASR, with some unique challenges
 - It has to be done in real time
 - A high latency response is perceived as a False Negative
 - · It has to work with very limited computational resources
 - These models need to be able to run on the device itself (i.e., they are not run in the cloud)
 - It needs to have high Precision
 - · False Positives lead to a lot of user friction

Matthieu François - Simon Lebeaud - Nicolas Tirel

Goal

Wake Word Models: DeepKWS

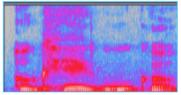
 The DeepKWS model used for Wake Word detection was released in 2014: Small-Footprint Keyword Spotting Using Deep Neural Networs



CNN

Wake Word Detection as Image Classification

- The input LFBE features to the DeepKWS model can be thought of as an image!
- This means we can try to use image classification techniques to try and solve the Wake Word detection problem.
 - Image Classification → Convolutional Neural Networks!



LBFE Features

Matthieu François - Simon Lebeaud - Nicolas Tirel

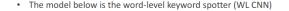
DeepLearn School - Guimaraes

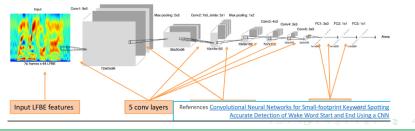
GreenAI U.P.P.A.

CNN

Wake Word Detection Models using CNNs

- It was shown that using Convolutional Neural Networks (CNNs) can improve Wake Word detection even more (Google showed a ~40% improvement over DeepKWS).
 - These models are attractive in a limited resource setting as the computational complexity can be easily controlled by adjusting various hyperparameters (e.g., kernel size, pooling size, and stride)





Matthieu François - Simon Lebeaud - Nicolas Tirel

GreenAI U.P.P.A.

Challenges

Wake Word Detection Challenges

- The models need to be able to run with very limited computational resources (in terms of compute power, available memory, and power constraints).
 - Model quantization (even down to 4 bits!), knowledge distillation, and pruning are all effective ways build effective models in this setting.
- The Wake Word needs to be detected in a far-field, noisy environment.
 - Robustness training is key! Augmenting training data with noise perturbations added to the input signals is a common way to improve performance.
 - Automatic Gain Control (AGC) can applied to the input where the signal is amplified whenever speech is detected.
 - Beam forming (using a microphone array to identifying the direction of the sound) can also be used to identify background noise.
 - When the direction of the signal jumps round \rightarrow it's probably noise

A comprehensive reference on KWS148

reenALU.P.P.A.

Matthieu François - Simon Lebeaud - Nicolas Tire

DeepLearn 2022 Spring

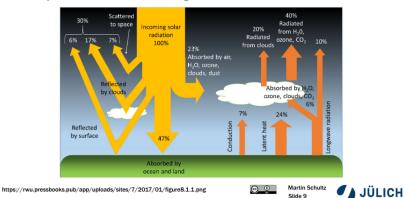
2 Graph Lecture

Biometrics Trustworthiness

4 Medicine, high physics and Weather Sofia Vallecorsa- Generative Models in High Energy Physics: Examples from CERN Lucila Ohno-machado - Use of Predictive Models in Medicine and Biomedical Research Rylan Conway - Deep Learning for Digital Assistants Martin Schultz - Deep Learning for Air Quality, Weather and Climate

Introduction

Atmospheric radiation budget



Matthieu François - Simon Lebeaud - Nicolas Tirel

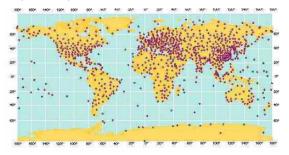
DeepLearn School - Guimaraes

GreenAI U.P.P.A.

Data

Global weather observations: vertical profiles

According to WMO (~1,300 sites)



Map from https://public.wmo.int/en/programmes/global-observing-system



Martin Schultz Slide 24



1atthieu François - Simon Lebeaud - Nicolas Tir

DeepLearn School - Guimaraes

GreenAI U.P.P.A.

One application, weather forecasting

Machine learning approaches to weather forecasting

Forecast problem

 $\mathbf{x}(t)
ightarrow \mathbf{x}(t+\Delta t)$

 $\mathbf{x}(t)$: State of the atmosphere at time t $\mathbf{x}(t+\Delta t)$: Forecast of atmospheric state at lead time Δt

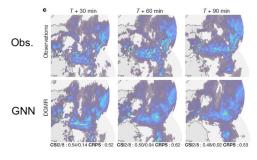


Matthieu François - Simon Lebeaud - Nicolas Tirel

One application, weather forecasting

NN Weather Forecasting

Precipitation nowcasting with radar data



Ravuri et al. (2021), Nature https://doi.org/10.1038/s41586-021-03854-z

30, 60, and 90 minute forecasts of a complex precipitation event over Scotland (24 June 2019, 15:15 UTC)

In a case study, 90% of meteorologists chose output from generative model over other methods.



Martin Schultz Slide 4



GreenAI U.P.P.A

Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn 2022 Spring

2 Graph Lecture

- **3** Biometrics Trustworthiness
- 4 Medicine, high physics and Weather

5 Ecology survey

- ・ロト ・回 ト ・ヨト ・ヨト ・ヨー うへで

Matthieu François - Simon Lebeaud - Nicolas Tirel

Questions (21 answers)

- How much are you aware of climate change?
- Is climate change caused by humans?
- Do you know IPCC?
- Do you know Labos 1Point5/carbon footprint calculator?
- What was your main means of transport to go to Guimaraes?

Natural change ?

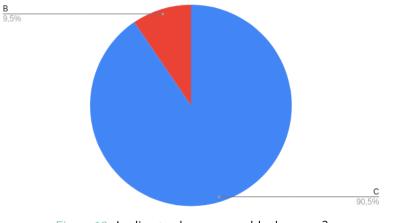
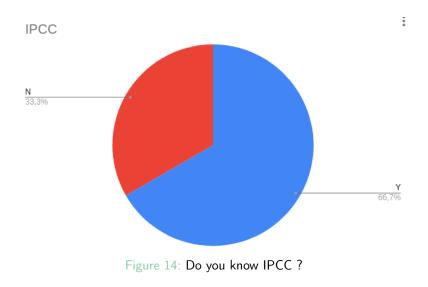


Figure 13: Is climate change caused by humans ?

 Matthieu François - Simon Lebeaud - Nicolas Tirel
 GreenAI U.P.P.A.

 DeepLearn School - Guimaraes
 76 / 80





- * ロ * * 個 * * 目 * * 目 * ・ 目 * うくや

Matthieu François - Simon Lebeaud - Nicolas Tirel

How much do you know about IPCC ?

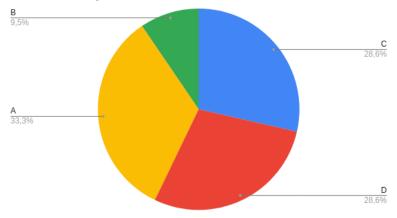
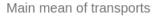


Figure 15: How much do you know about it ?

	· · · · · ·	Simon Lebeaud - Nicolas Tirel
DeepLear	n School -	Guimaraes

GreenAI U.P.P.A.



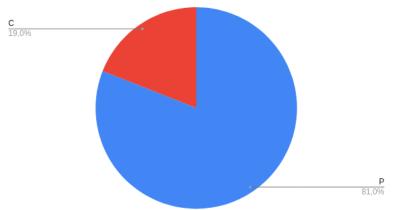
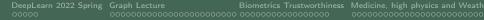
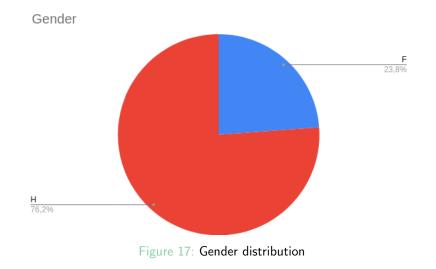


Figure 16: What was your main means of transport to go to Guimaraes ?





Matthieu François - Simon Lebeaud - Nicolas Tirel

DeepLearn School - Guimaraes

GreenAI U.P.P.A.