Deep Representations

Frederic Precioso

Université Nice Sophia Antipolis
Membre de UNIVERSITÉ CÔTE D'AZUR

cnrs

i3s sophia antipolis

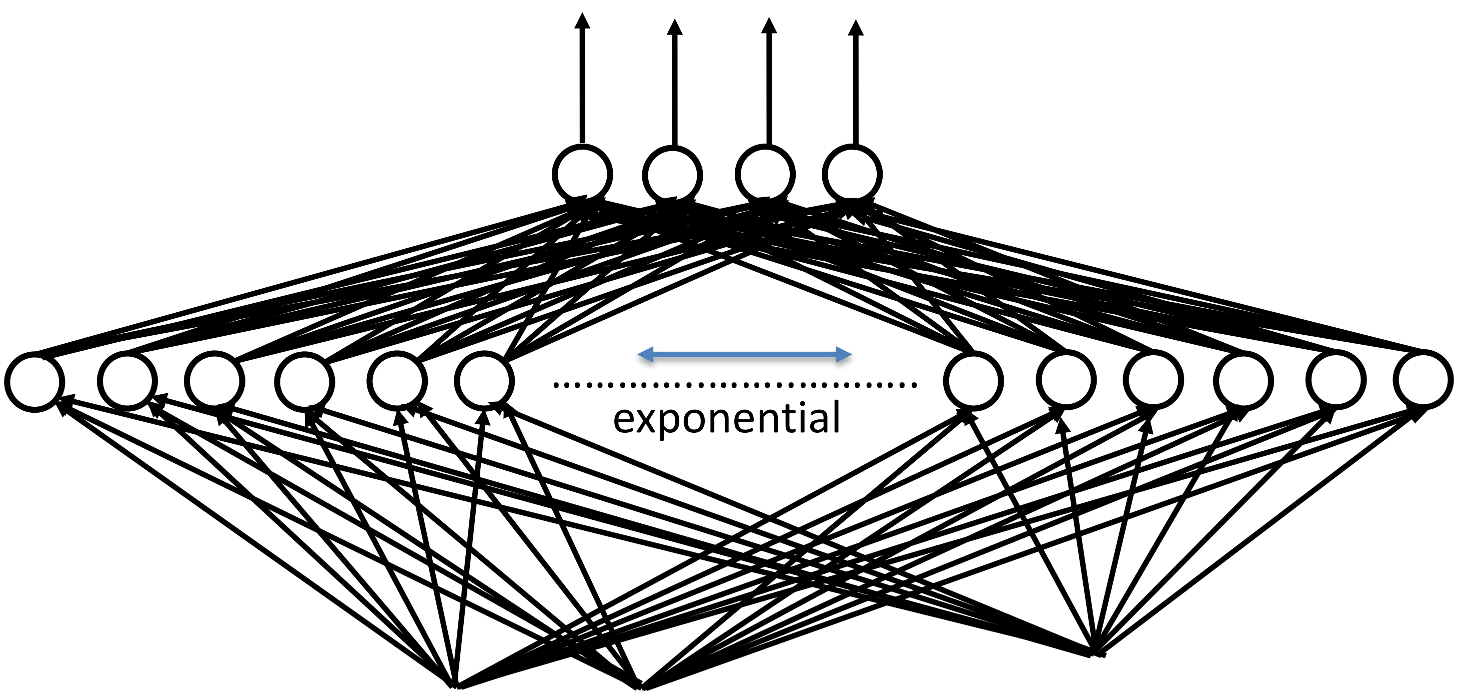
Disclaimer

If any content in this presentation is yours but is not correctly referenced or if it should be removed, please just let me know and I will correct it.

DEEP NETWORKS

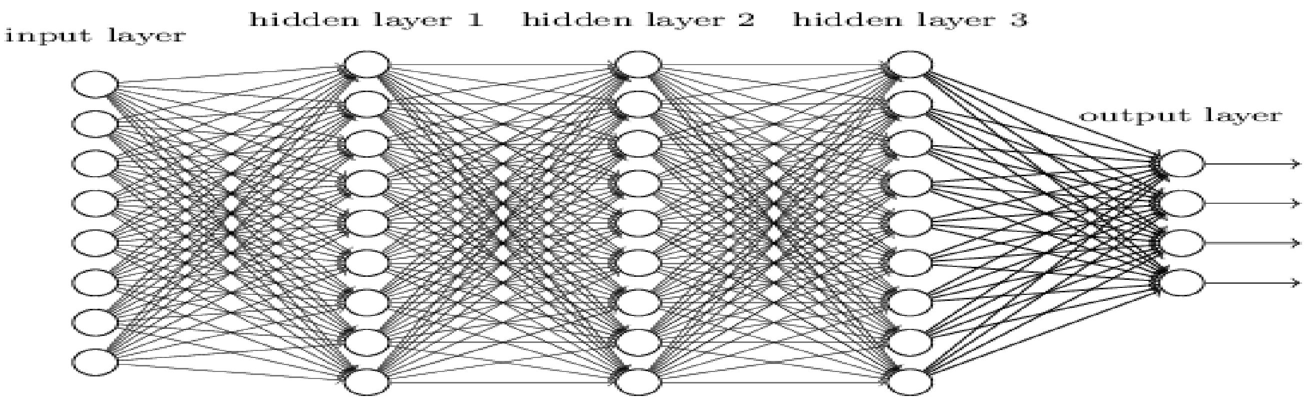
Deep representation origins

- **Theorem Cybenko** (1989) *A neural network with one single hidden layer is a universal "approximator", it can represent any continuous function on compact subsets of* $\mathbf{R}^n \Rightarrow$ *2 layers are enough…but hidden layer size may be exponential*



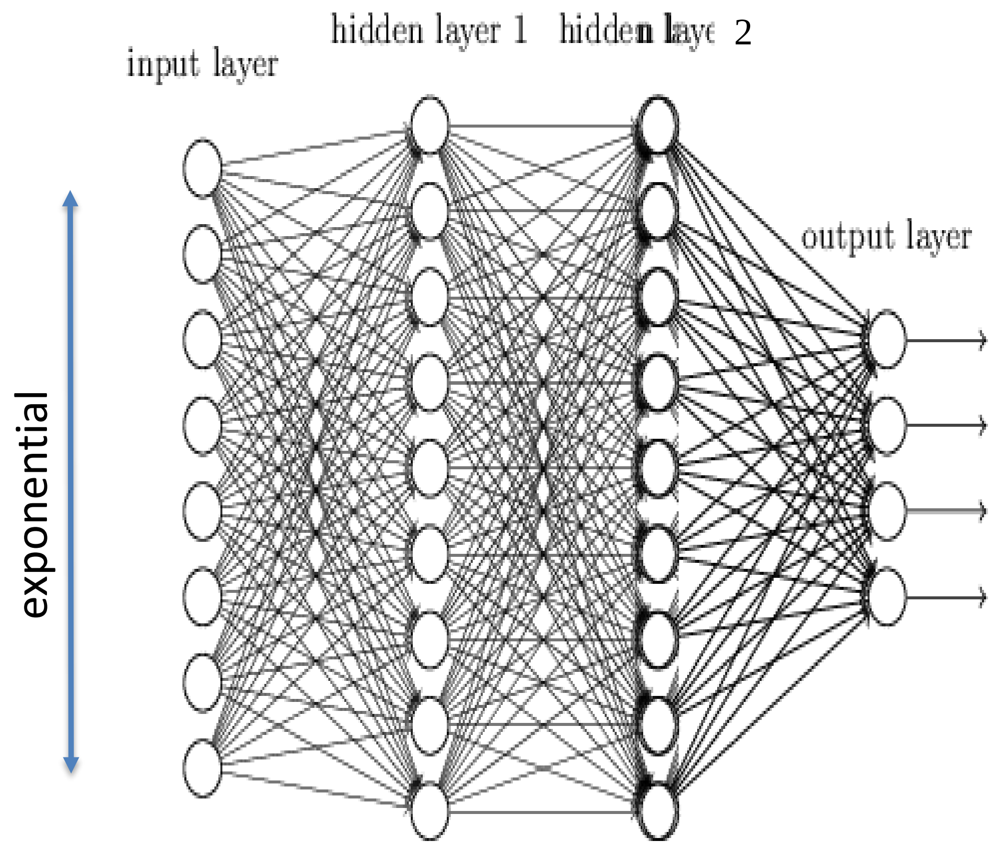
Deep representation origins

- **Theorem Hastad** (1986), **Bengio** et al. (2007) Functions representable compactly with *k* layers may require exponentially size with *k-1* layers



Deep representation origins

- **Theorem Hastad** (1986), **Bengio** et al. (2007) Functions representable compactly with *k* layers may require exponentially size with *k-1* layers



Enabling factors

- Why do it now ? Before 2006, training deep networks was unsucessfull because of practical aspects
  - faster CPU's
  - parallel CPU architectures
  - advent of GPU computing

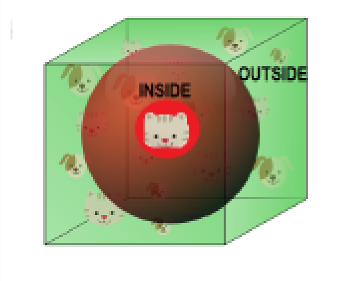
- Hinton, Osindero & Teh « A Fast Learning Algorithm for Deep Belief Nets », *Neural Computation*, 2006
- Bengio, Lamblin, Popovici, Larochelle « Greedy Layer-Wise Training of Deep Networks », *NIPS'2006*
- Ranzato, Poultney, Chopra, LeCun « Efficient Learning of Sparse Representations with an Energy-Based Model », *NIPS'2006*

The curse of dimensionality [Bellman, 1956]

UNIVERSITÉ CÔTE D'AZUR
univ-cotedazur.fr

- Euclidian distance is not relevant in high dimension: d $\geq$10
  1. look at the examples at distance at most r
  2. the hypersphere volume is too small: practically empty of examples

$$\frac{volume\ of\ \ the\ sphere\ of\ \ radial\ r}{hypersphere\ of\ \ 2r\ \ width} \rightarrow_{d\rightarrow\infty} 0$$



  3. need a number of examples exponential in d

Remark

Specific care for data representation

Blessing of dimensionality: Thomas Cover's Theorem (1965)

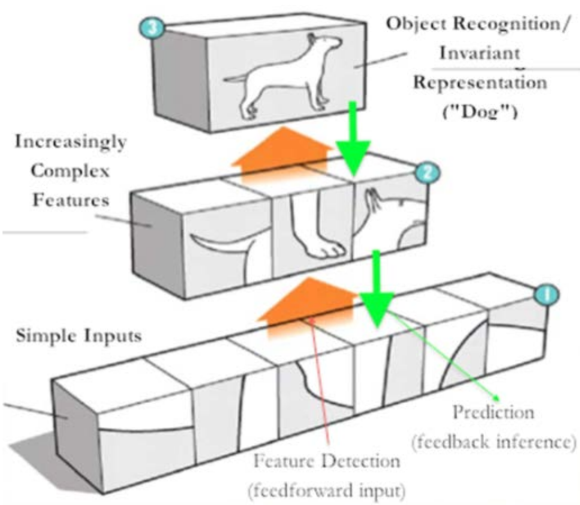
Cover's theorem states: A complex pattern-classification problem cast in a high-dimensional space nonlinearly is more likely to be linearly separable than in a low-dimensional space (repeated sequence of Bernoulli trials).

The number of groupings that can be formed by (l-1)-dimensional hyperplanes to separate N points in two classes is

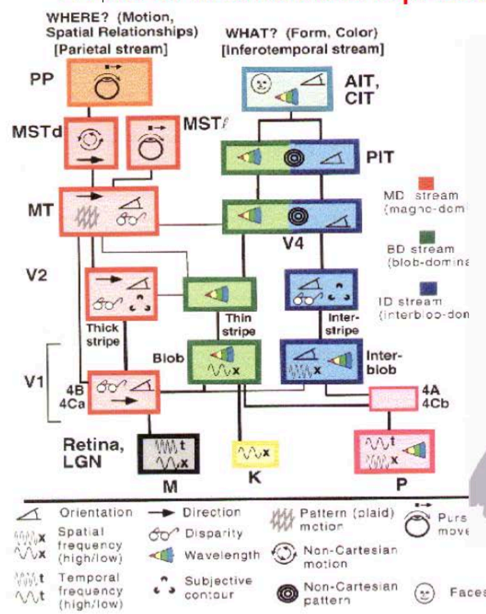
$$O(N,l) = 2\sum_{i=0}^{l} \frac{(N-1)!}{(N-1-i)!\,i!}$$

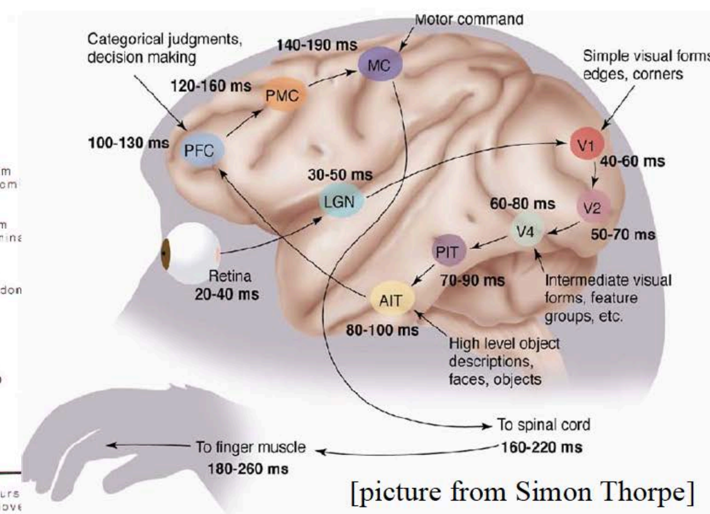
Convolutional Neural Networks (aka CNN, ConvNet)

The Mammalian Visual Cortex Inspires CNN



- The ventral (recognition) pathway in the visual cortex has multiple stages
- Retina - LGN - V1 - V2 - V4 - PIT - AIT ....
- Lots of intermediate representations



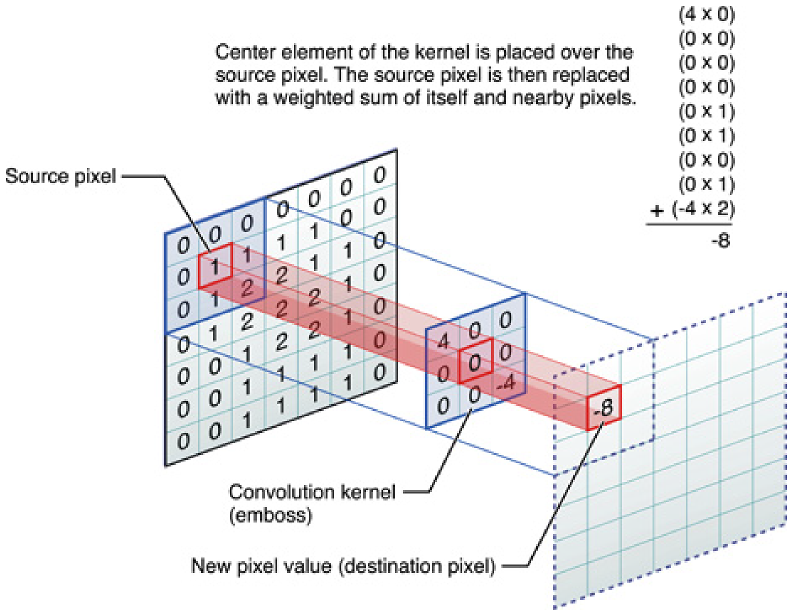


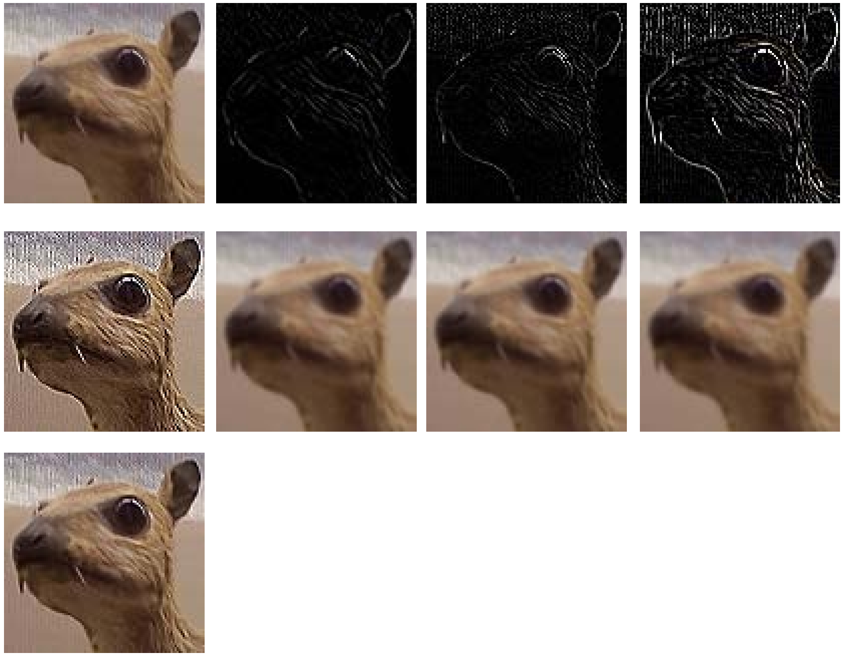
[Gallant & Van Essen]

UNIVERSITÉ CÔTE D'AZUR

univ-cotedazur.fr

Deep representation by CNN

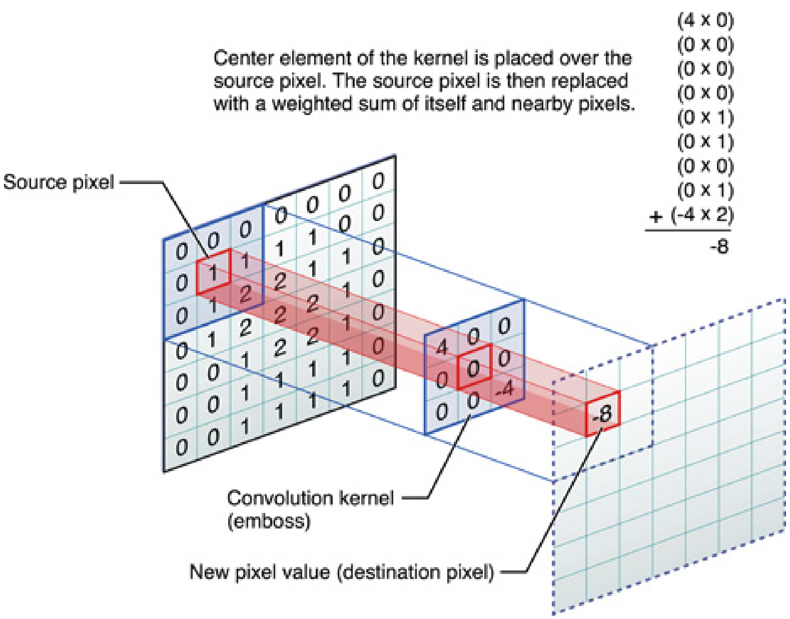


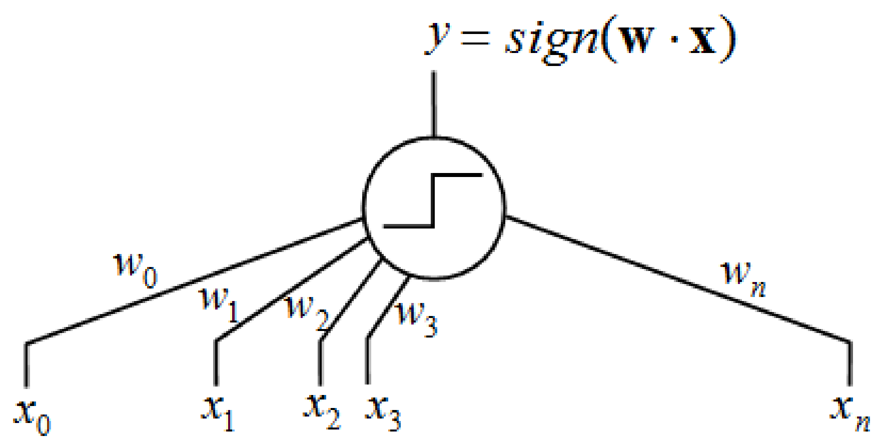


UNIVERSITÉ CÔTE D'AZUR

univ-cotedazur.fr

Deep representation by CNN



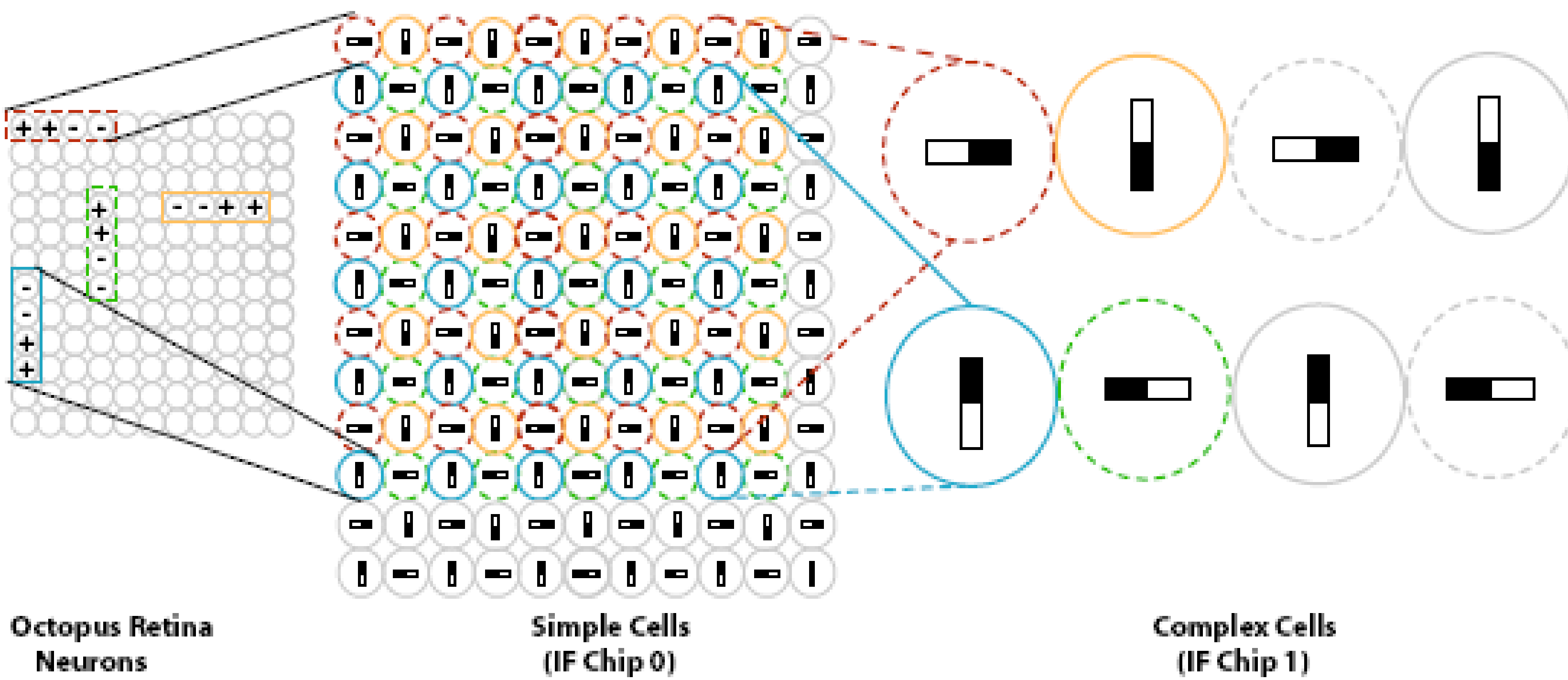


Deep representation by CNN

A cell is related to a subpart of the field of vision

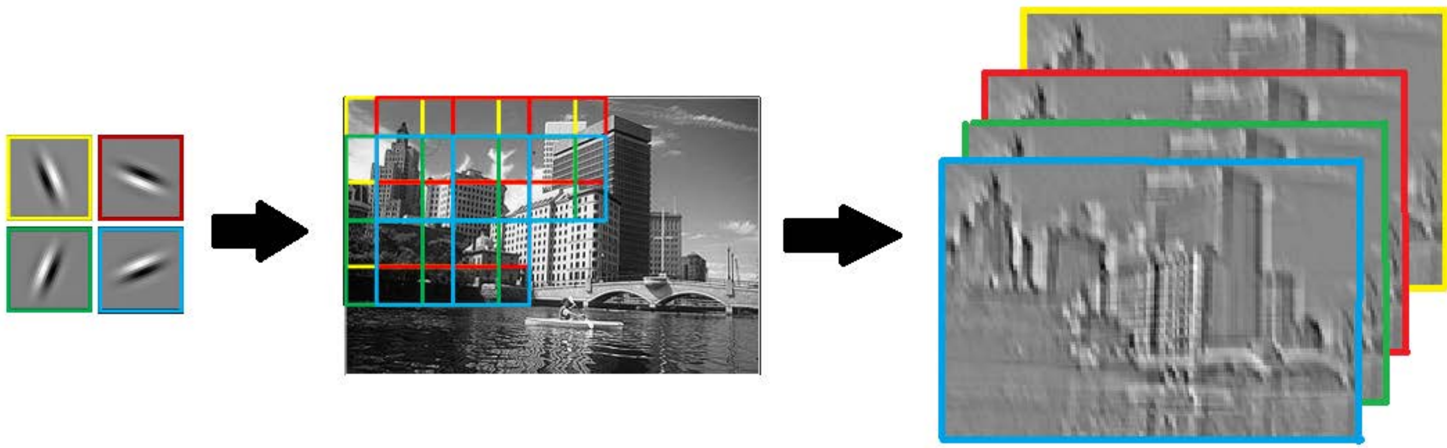
Two main kind of cells:

1) S cells: extract the characteristics
2) C cells: assemble the characteristics



Deep representation by CNN

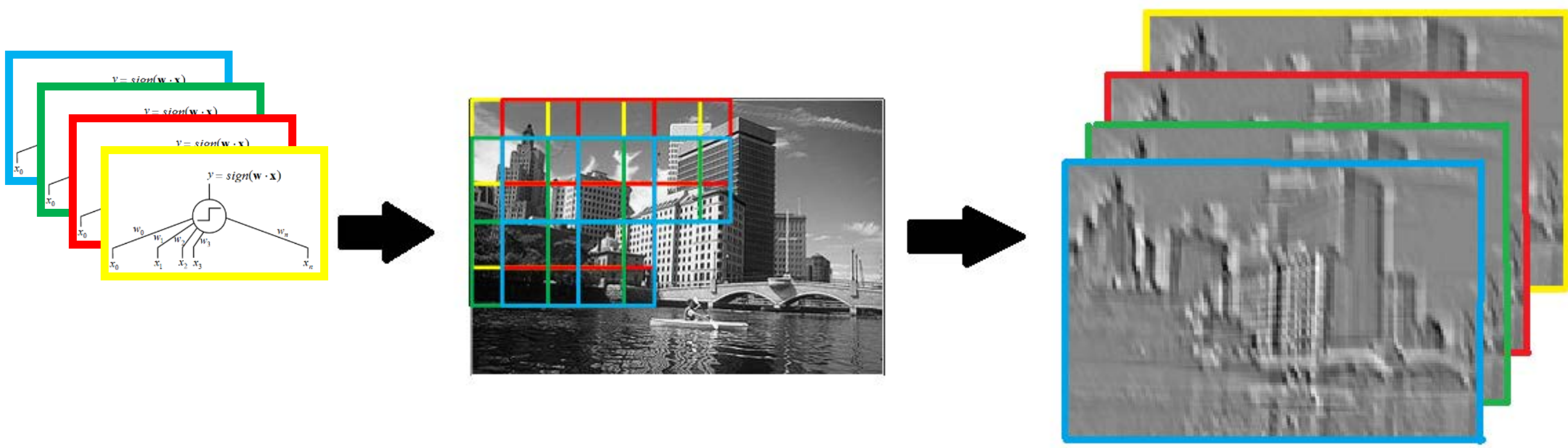
1. Hubel et Wiesel's work on cat's visual cells (1962)
2. Convolution



3. Max Pooling

Deep representation by CNN

1. Hubel et Wiesel's work on cat's visual cells (1962)
2. Convolution

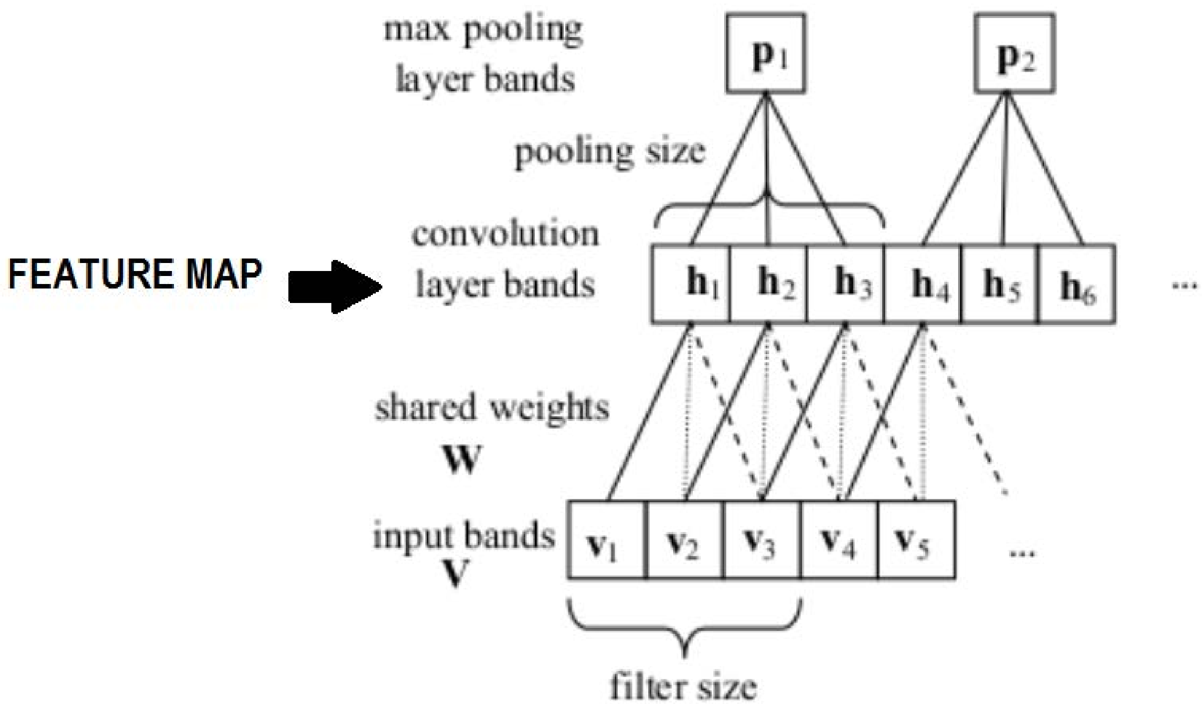


3. Max Pooling

Deep representation by CNN

Yann Lecun, [LeCun et al., 1998]

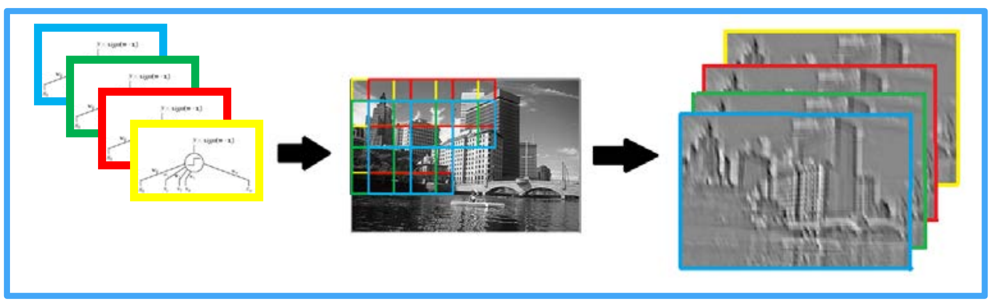
1. Subpart of the field of vision and translation invariant
2. S cells: convolution with filters
3. C cells: max pooling

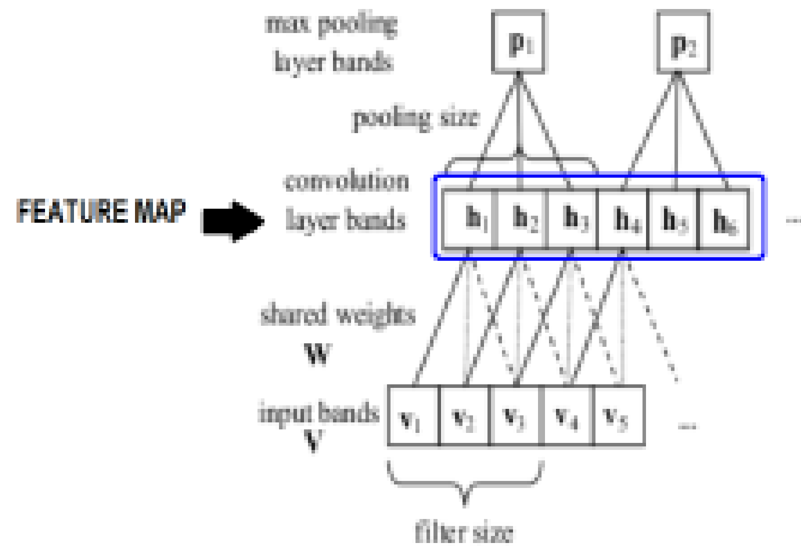


Deep representation by CNN

Yann Lecun, [LeCun et al., 1998]

1. Subpart of the field of vision and translation invariant
2. S cells: convolution with filters
3. C cells: max pooling





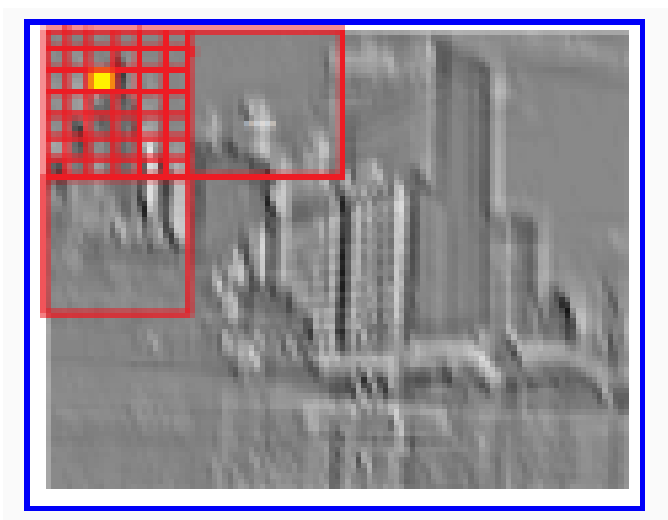
UNIVERSITÉ CÔTE D'AZUR

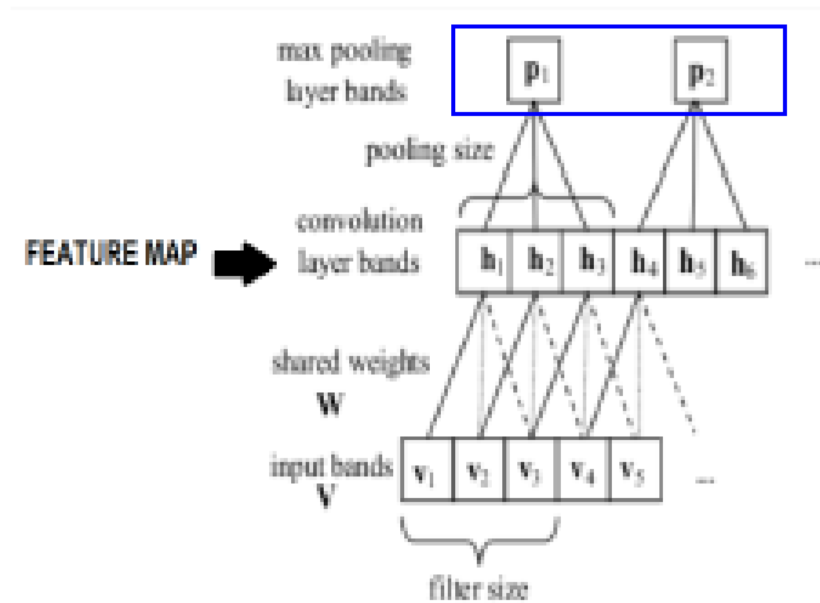
univ-cotedazur.fr

Deep representation by CNN

Yann Lecun, [LeCun et al., 1998]

1. Subpart of the field of vision and translation invariant
2. S cells: convolution with filters
3. C cells: max pooling



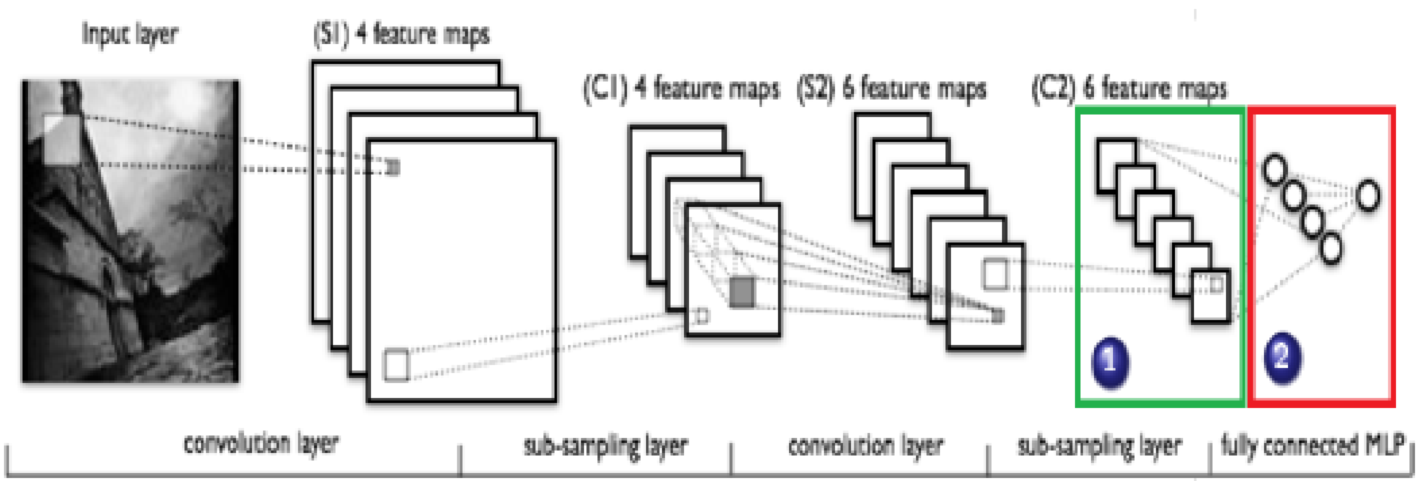


UNIVERSITÉ CÔTE D'AZUR

univ-cotedazur.fr

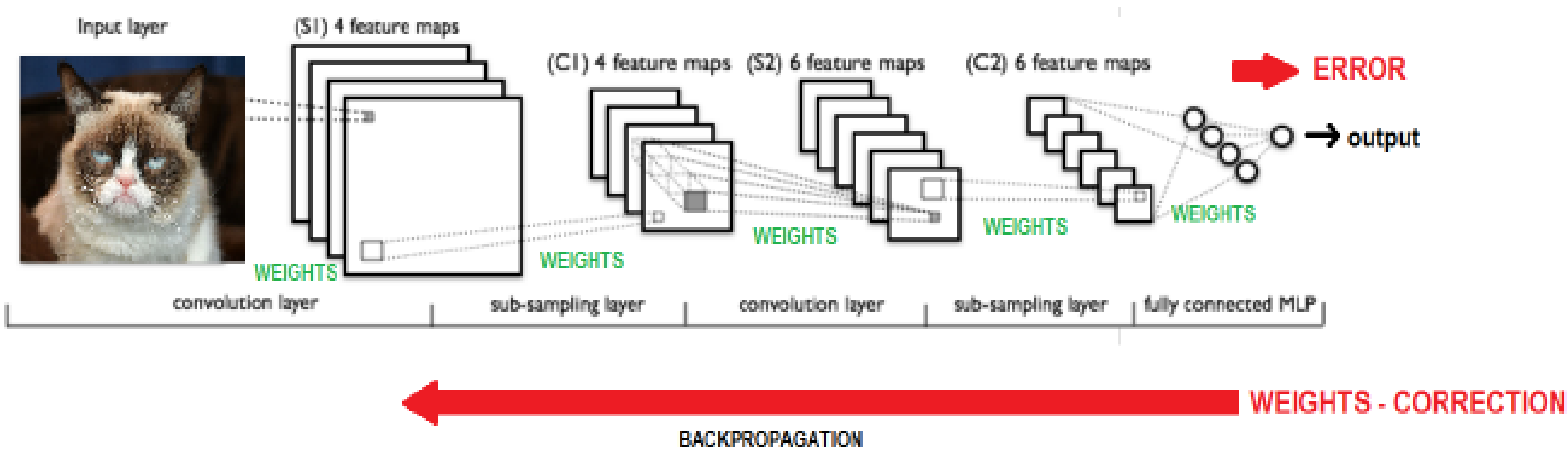
Deep representation by CNN

- feature map = result of the convolution
- convolution with a filter extract characteristics (*edge detectors*)
- extract parallelised characteristics at each layer



1. final representation of our data
2. classifier (MLP)

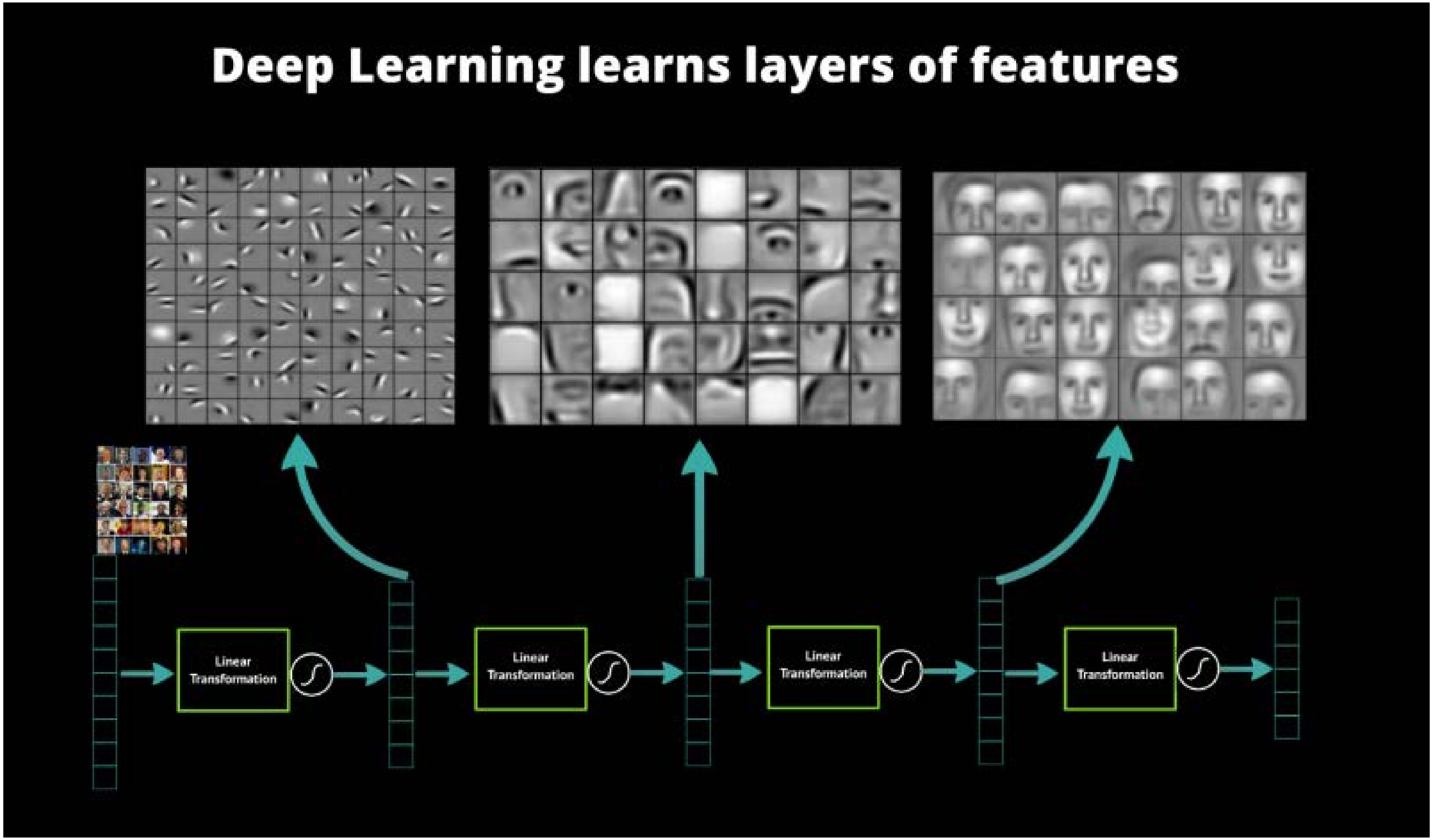
Deep representation by CNN



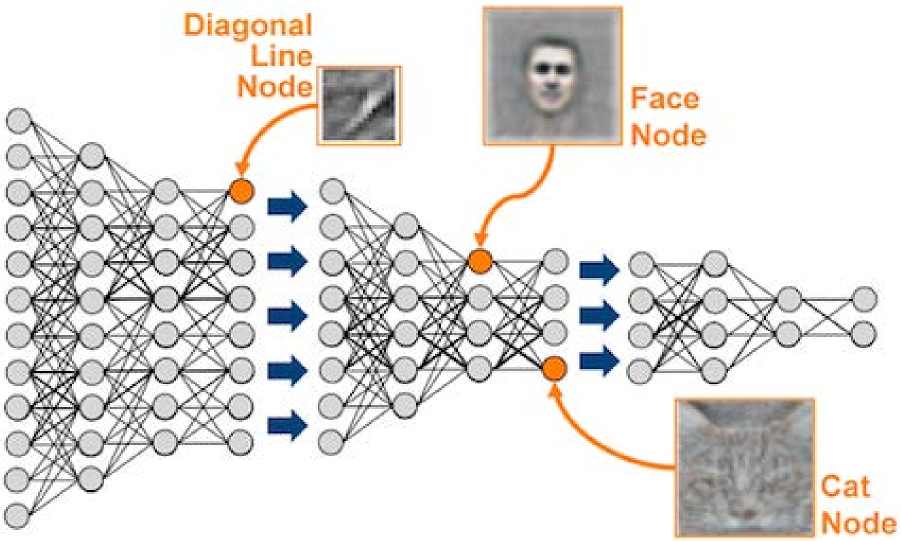
UNIVERSITÉ CÔTE D'AZUR

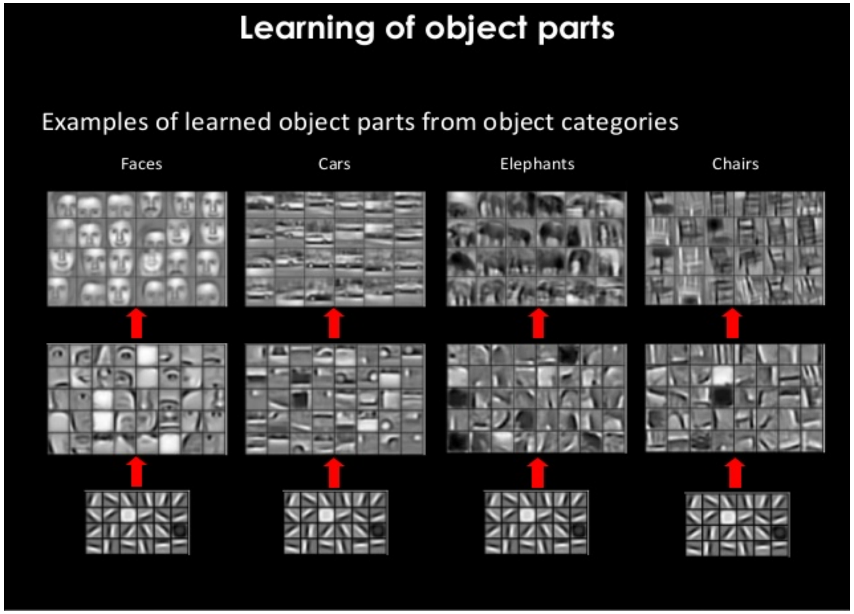
univ-cotedazur.fr

Deep representation by CNN



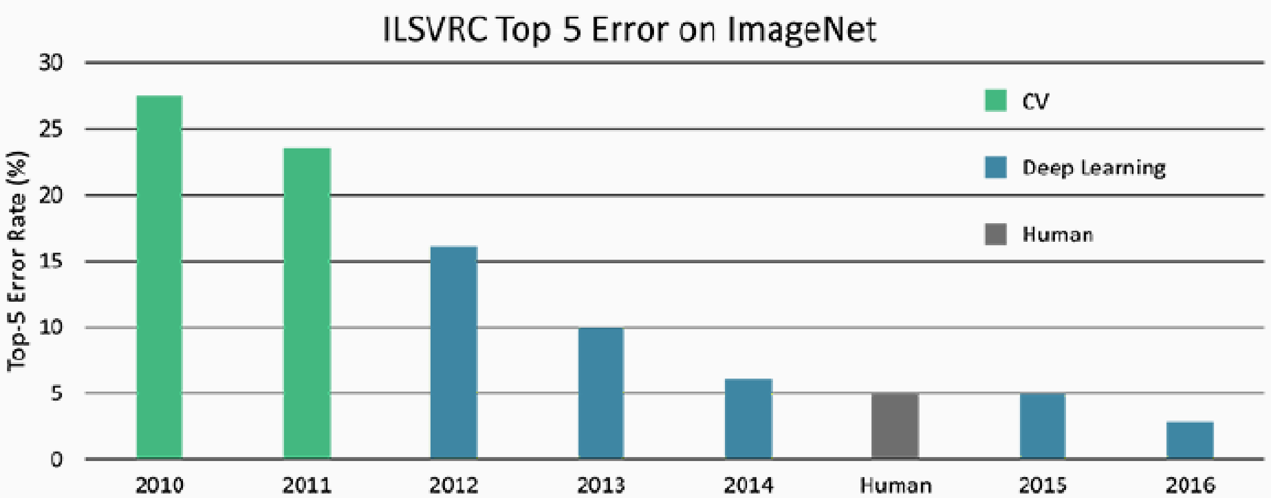
Deep representation by CNN





Deep representation by CNN

- Deep Networks are as good as humans at recognition, identification...

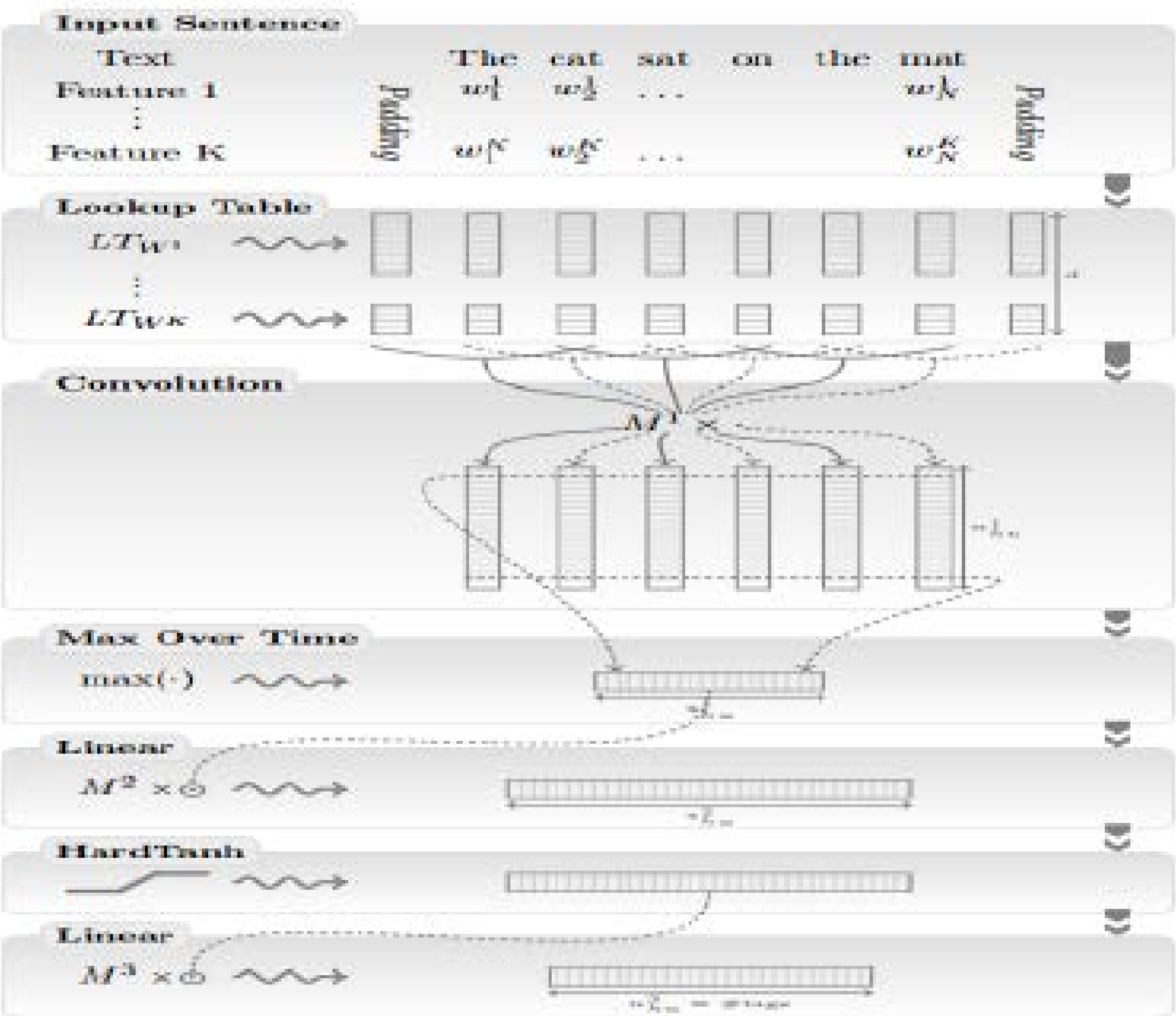


How much does a deep network understands those tasks?

Deep representation by CNN

Convolutional Neural Networks Extensions

Deep representation by CNN



R. Collobert, J. Weston, L. Bottou, M. Karlen, K. Kavukcuoglu and P. Kuksa. Natural Language Processing (Almost) from Scratch. Journal of Machine Learning Research, 12:2493-2537, 2011.

Deep representation by CNN

Task	Benchmark	Collobert
Part of Speech	97.24%	97.29%
Chunking	94.29%	94.32%
Named Entity Recognition	77.92%	75.49%
Semantic Role Labeling	89.31%	89.59%

Collobert is working quite well but:

1. 852 million words
2. 4 weeks

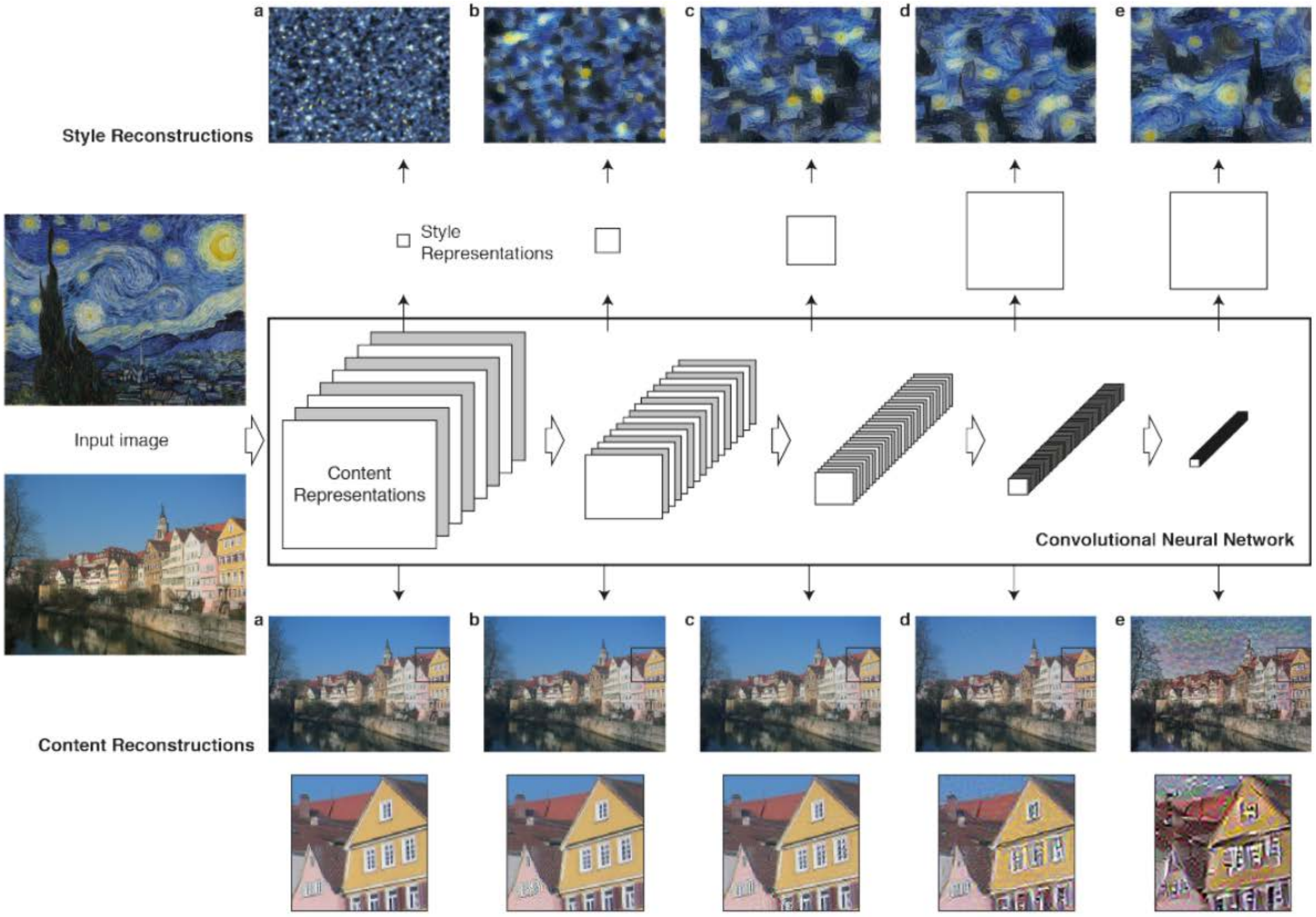
L. A. Gatys, A. S. Ecker, and M. Bethge, “Image Style Transfer Using Convolutional Neural Networks”, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2016

Combining the Content of one image with the style of an artwork using a CNN

UNIVERSITÉ CÔTE D'AZUR

univ-cotedazur.fr

Separation of Content and Style



UNIVERSITÉ CÔTE D'AZUR

univ-cotedazur.fr

Separate Content from Artwork

- Use intermediate layers of CNN
- Perform gradient-descent on white noise image to match the content
- Squared-error loss between two feature representations (F: generated image, P: original image)

$$\mathcal{L}_{content}(\vec{p}, \vec{x}, l) = \frac{1}{2} \sum_{i,j} \left(F_{ij}^l - P_{ij}^l\right)^2$$

- Derivative:

$$\frac{\partial \mathcal{L}_{content}}{\partial F_{ij}^l} = \begin{cases} \left(F^l - P^l\right)_{ij} & \text{if } F_{ij}^l > 0 \\ 0 & \text{if } F_{ij}^l < 0 \end{cases}$$

- Update until it matches the original image

Separate Style from Artwork

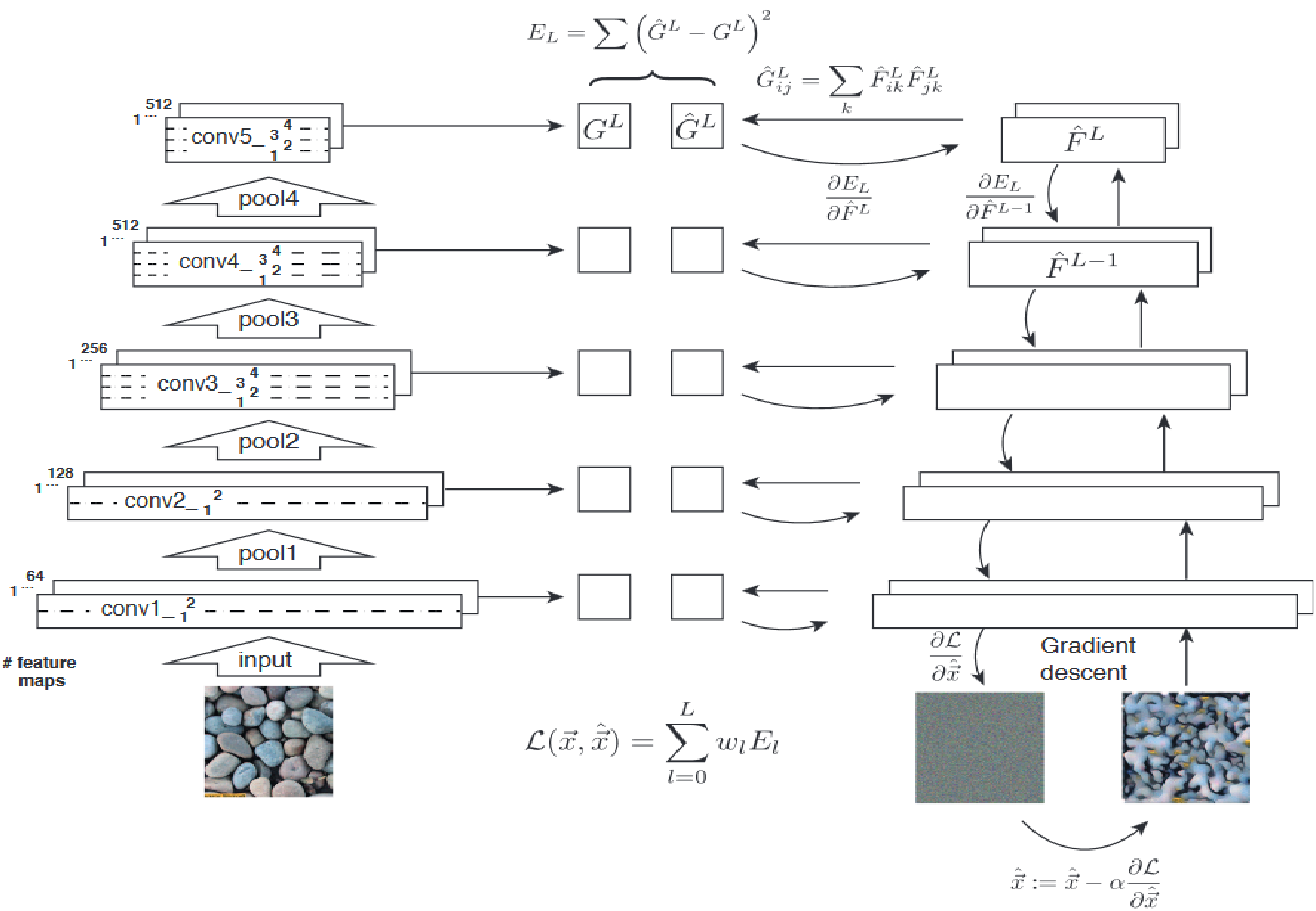
- Based on the paper "*Texture Synthesis Using Convolutional Neural Networks*"
- Objective: Calculate the correlation between different features
- Gram matrix:

$$G^l \in \mathcal{R}^{N_l \times N_l}$$

- Where G^l_{ij} is the inner product between the vectorized feature map *i* and *j* in layer *l*:

$$G^l_{ij} = \sum_k F^l_{ik} F^l_{jk}$$

Separate Style from Artwork



Generate a new image

Content representation

+

Style representation

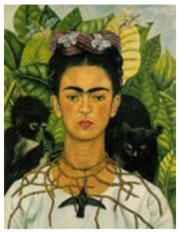
Generate a new image

- Minimize total loss function from white-noise image

$$\mathcal{L}_{total}(\vec{p}, \vec{a}, \vec{x}) = \alpha \mathcal{L}_{content}(\vec{p}, \vec{x}) + \beta \mathcal{L}_{style}(\vec{a}, \vec{x})$$

- α and β are weighting factors

Generate a new image












Transfer learning…

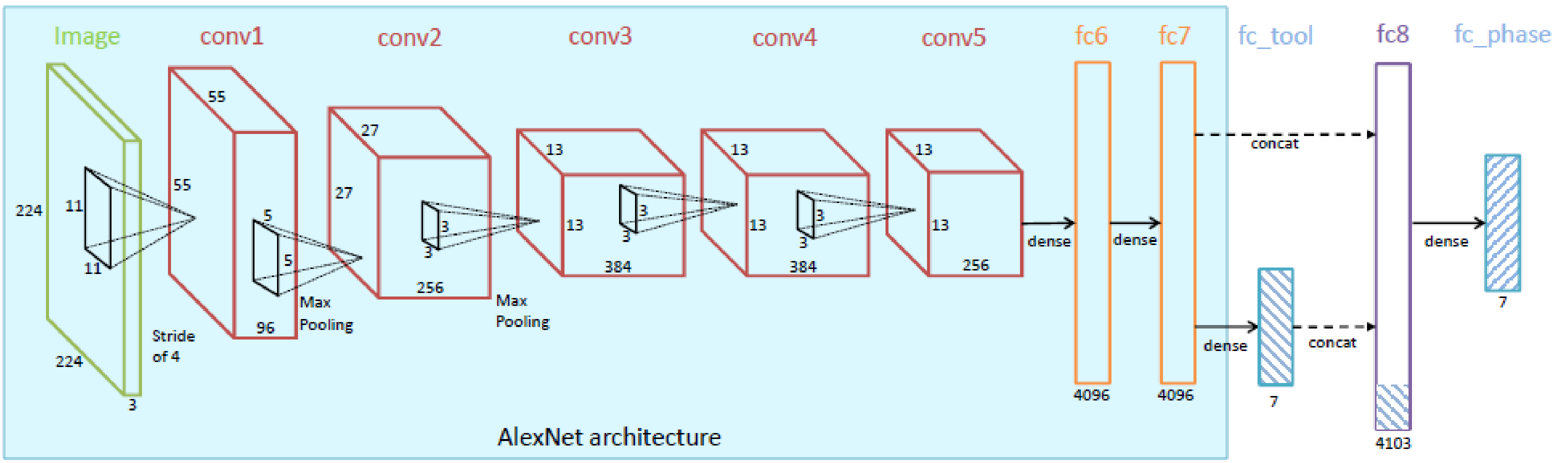


Fig. 2: EndoNet architecture (best seen in color). The layers shown in the turquoise rectangle are the same as in the AlexNet architecture.

ADVERSARIAL EXAMPLES

Amazing but…Adversary examples

Intriguing properties of neural networks

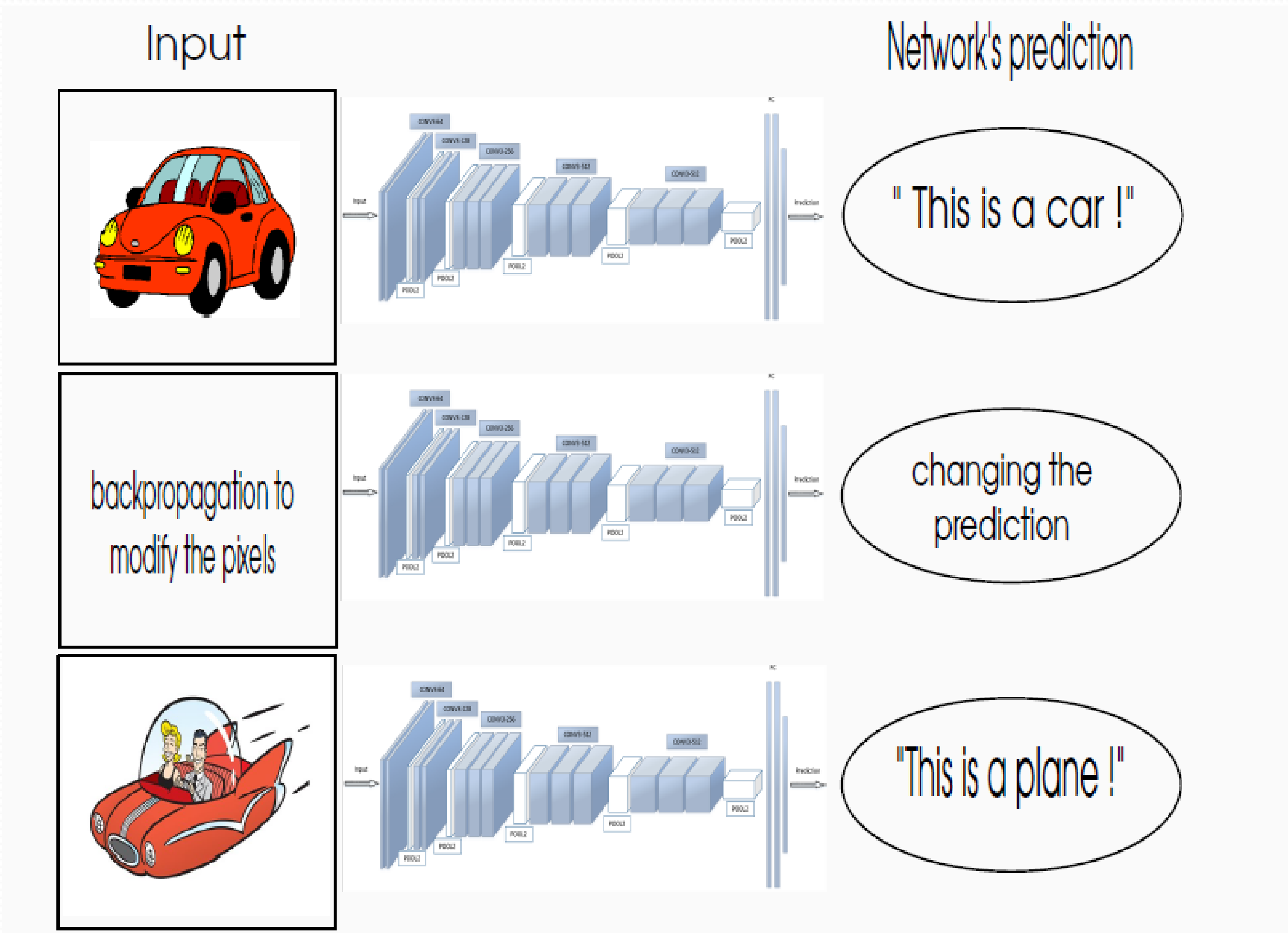
C. Szegedy, w. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, R. Fergus

arXiv preprint arXiv:1312.6199

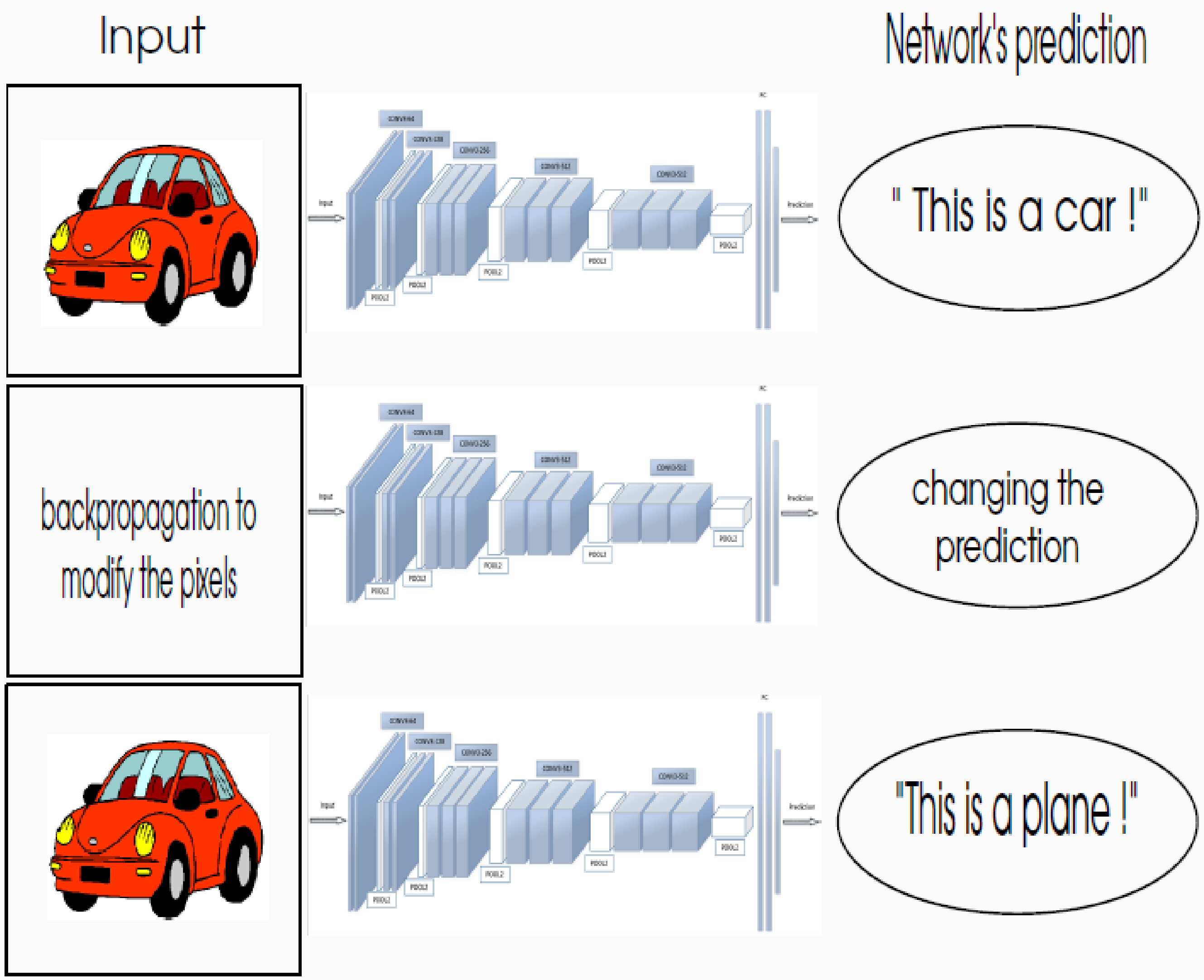
2013

[1312.6199] Intriguing properties of neural networks - arXiv.org
https://arxiv.org › cs - Traduire cette page
de C Szegedy - 2013 - Cité 449 fois - Autres articles
21 déc. 2013 - In this paper we report two such **properties**. First, we ... Second, we find that deep **neural networks** learn input-output mappings that are fairly ...

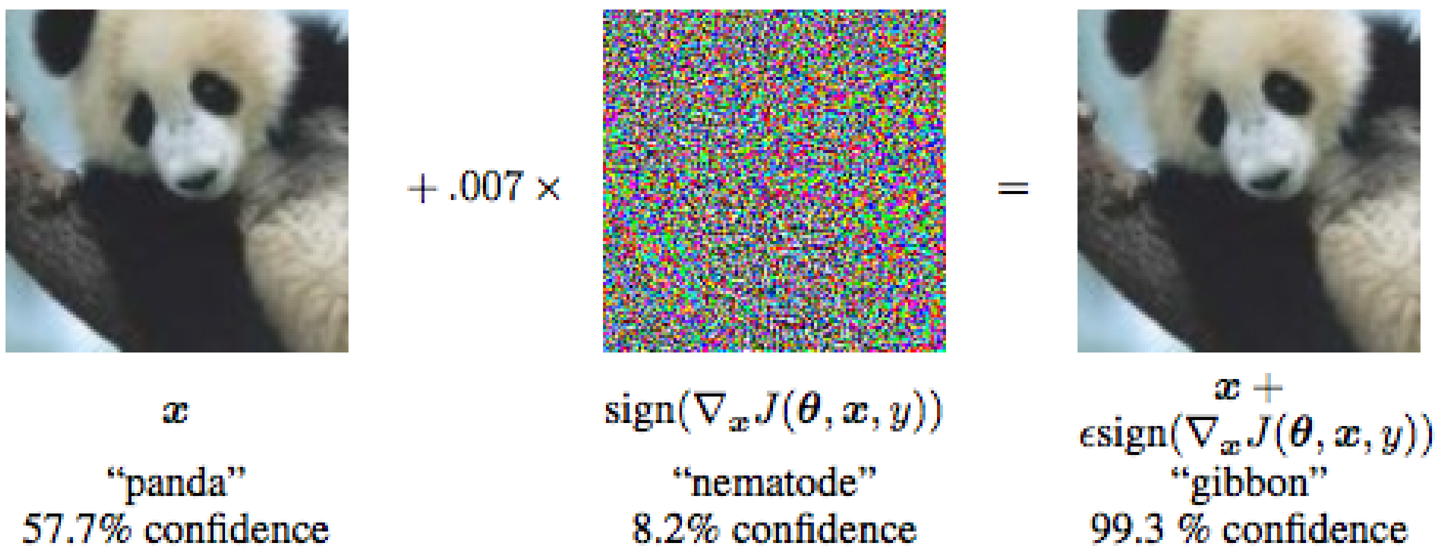
Amazing but…Adversary examples



Amazing but…Adversary examples

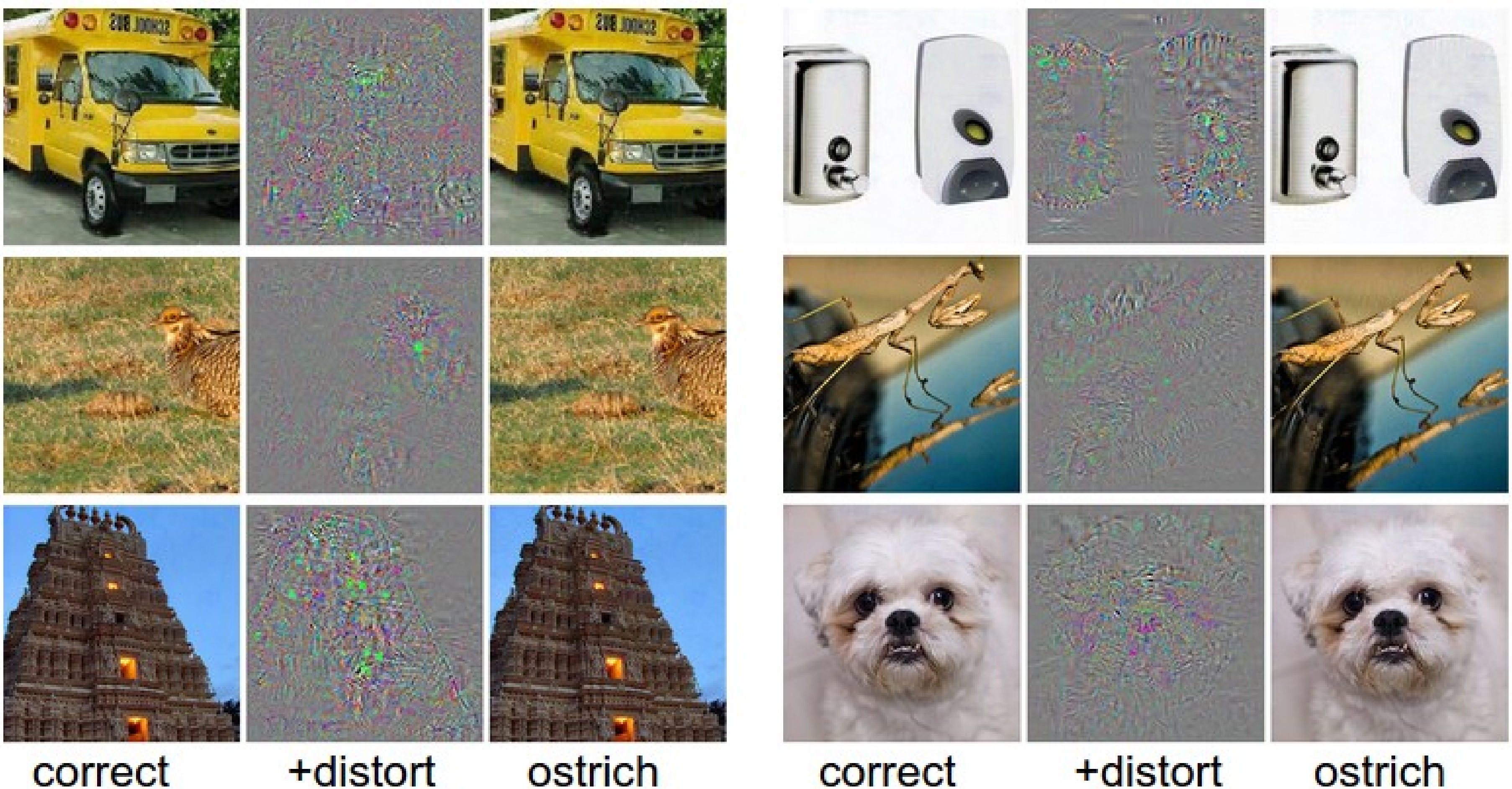


Amazing but…Adversary examples



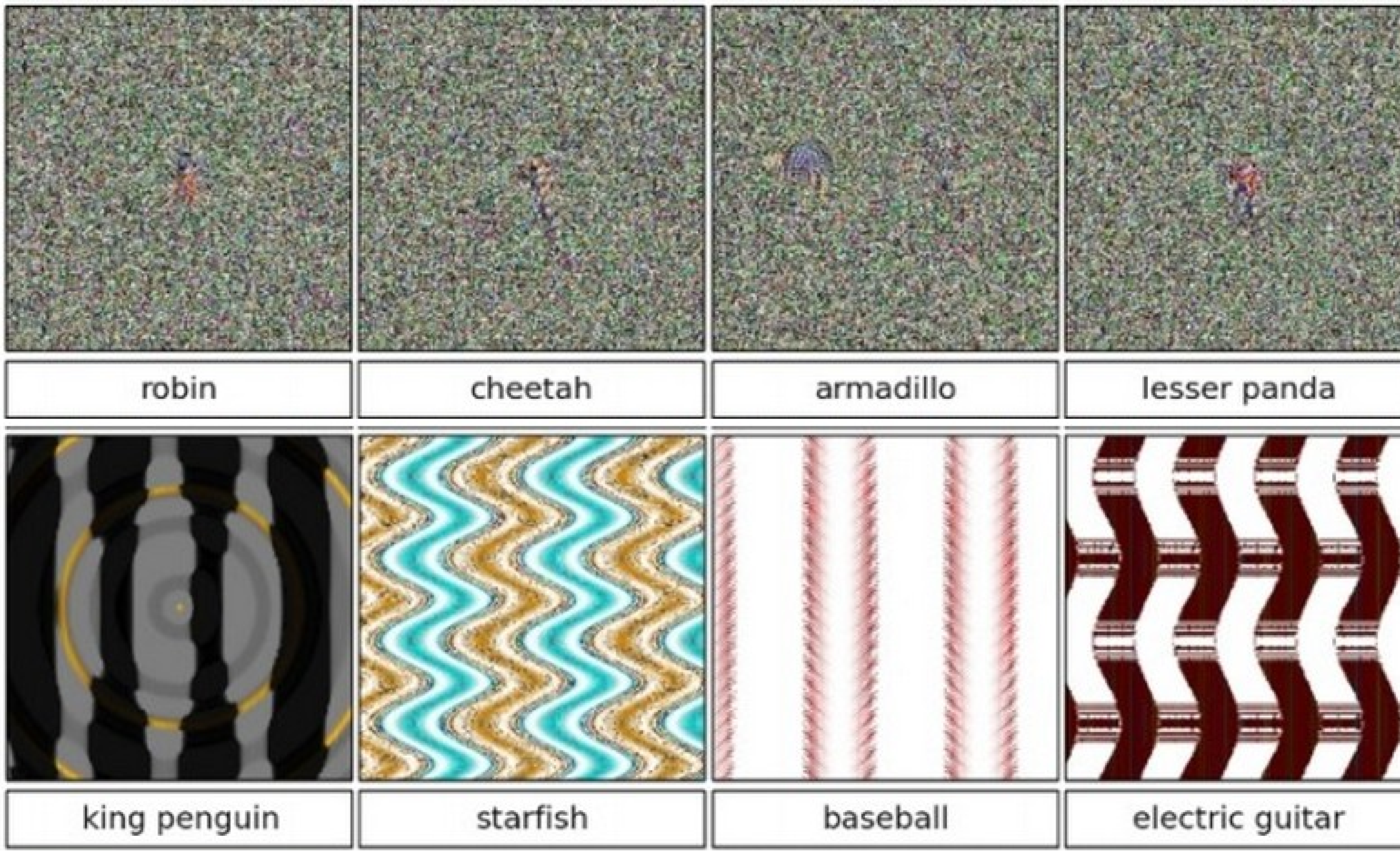
Andrej Karpathy blog, http://karpathy.github.io/2015/03/30/breaking-convnets/

Amazing but…Adversary examples



Andrej Karpathy blog, http://karpathy.github.io/2015/03/30/breaking-convnets/

Amazing but…Adversary examples



Andrej Karpathy blog, http://karpathy.github.io/2015/03/30/breaking-convnets/

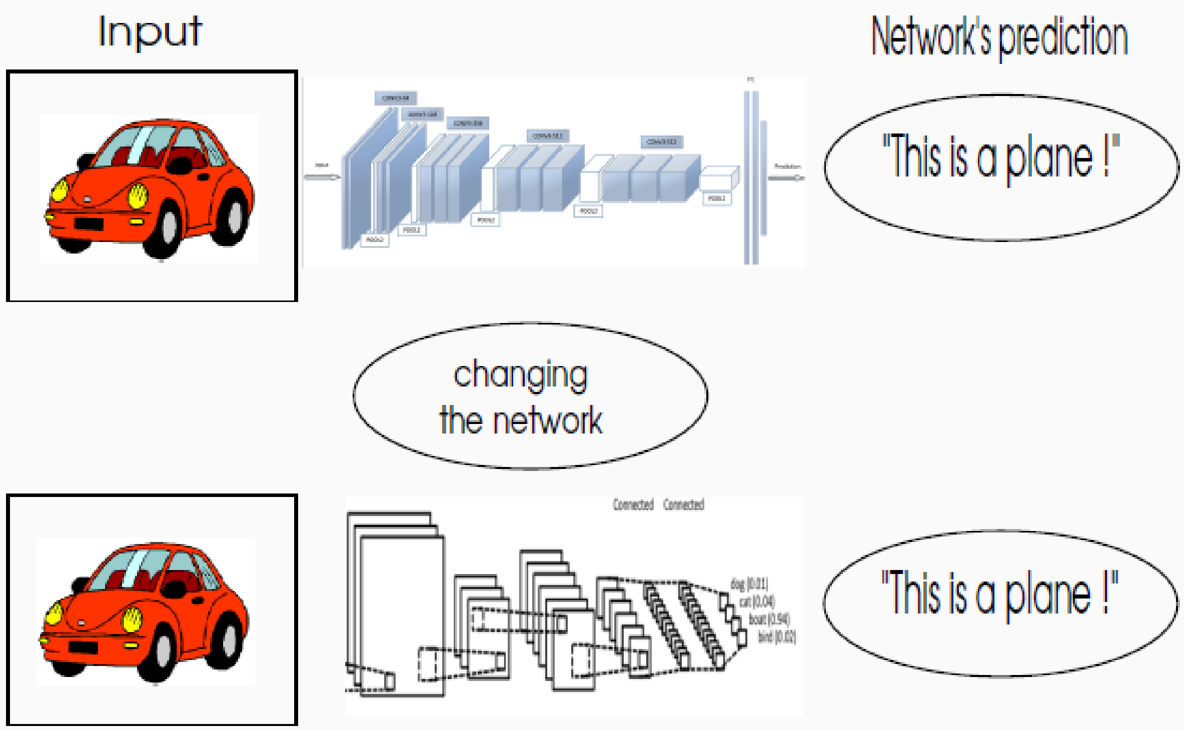
Amazing but…Adversary examples

Definition: $\hat{x}$ is called adversarial iff:

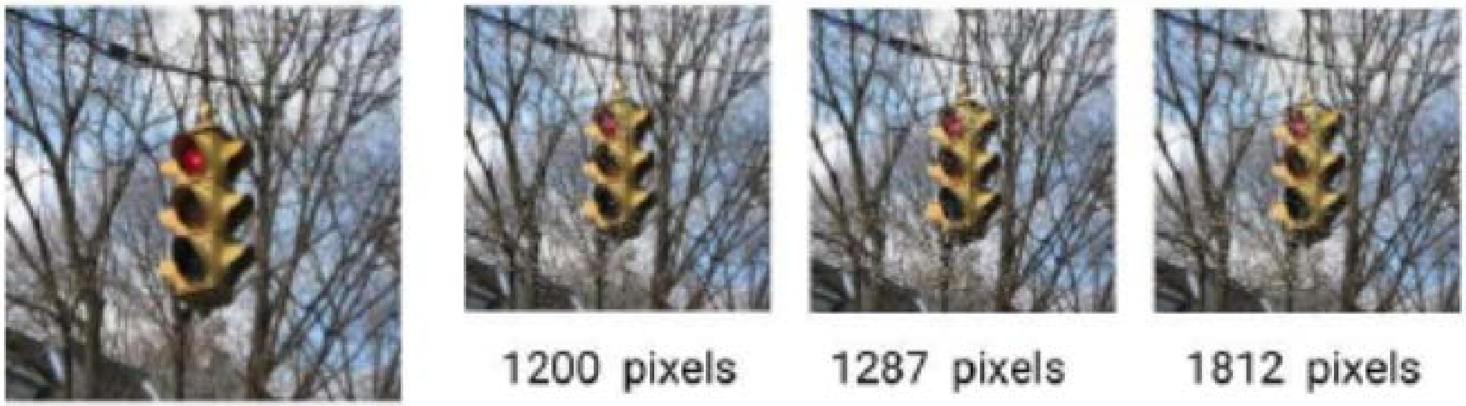
- given image x
- low distortion $\| x - \hat{x} \| < \epsilon, \quad (\epsilon > 0$, few pixels)
- given network's probabilities $f_\theta(x)$
- Different predictions! $argmaxf_\theta(x) \neq argmaxf_\theta(\hat{x})$

Amazing but...Adversary examples

- $\neq$ outliers
- regularization: correct one... find another
- high confidence predictions
- **Transferability**



Amazing but…Adversary examples

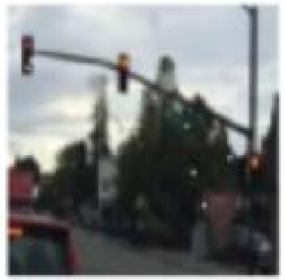


1200 pixels 1287 pixels 1812 pixels

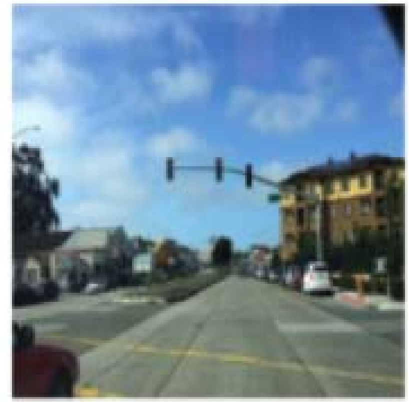
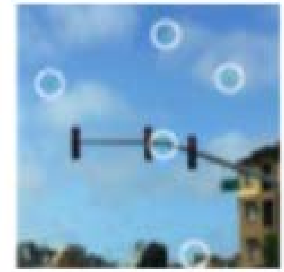
Original Traffic light (ImageNet class 920)	VGG16	VGG19 Misclassified	RESNET

State-of-the art deep neural networks on ImageNet

Amazing but…Adversary examples

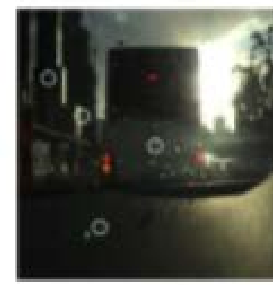



Red Light Modified to
Green after 18 white pixels.
Probability: 59%

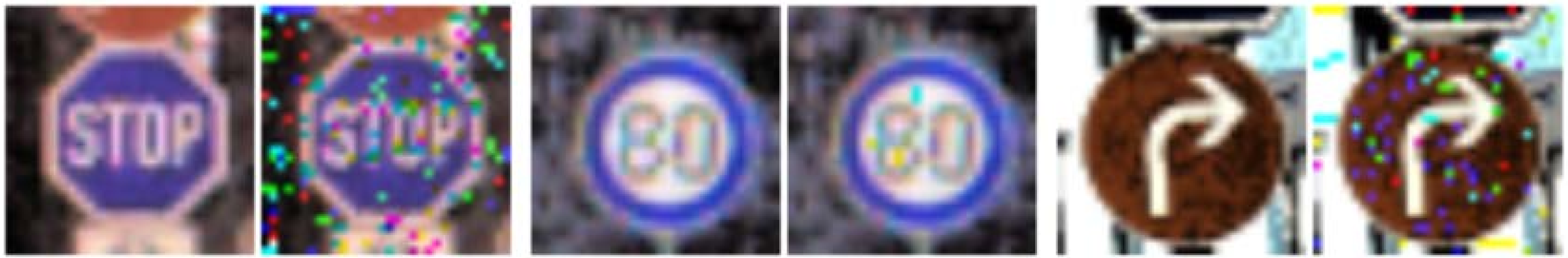
Red Light Modified to
Green after 9 green pixels.
Probability: 50.9%


Red Light Modified to
Green after 9 green pixels.
Probability: 53%

No Light Modified to Green
after 4 green pixels.
Probability: 51.9%

Amazing but…Adversary examples



stop	30m speed limit	80m speed limit	30m speed limit	go right	go straight

Confidence 0.999964 0.99

Super tuto adversarial examples

- A tutorial made by a MAM5 student: Guillaume Debard (promo 2017)
  - Slides here: http://www.telecom-valley.fr/wp-content/uploads/2017/05/DEBARD.pdf
  - Video here: https://www.youtube.com/watch?v=1wyXPY0VxTc