

# Rozpoznawanie w oparciu o algorytmy CNN. Steganografia

WYKŁAD 8  
Dla studiów niestacjonarnych  
2021/2022

Dr hab. Anna Korzyńska, prof. IBIB PAN

# Komputerowa analiza i rozpoznawanie obrazów



Jest to „sztuka” udzielania, **automatycznej** i mającej **matematyczne podstawy** odpowiedzi na pytanie:

**Co ten obraz przedstawia (i o czym mówi) ?**

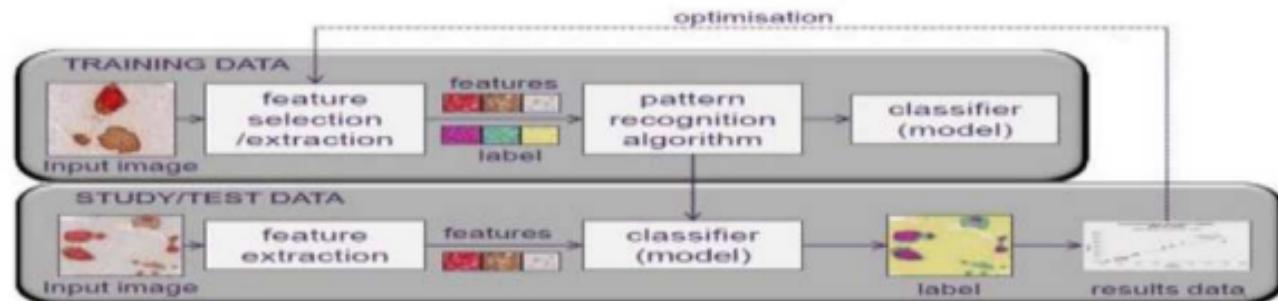
Podejścia:

1. **Klasyczna** – oparta o cechy dobranych przez deweloperów systemu na podstawie rad ekspertów i ich doświadczenia
  - **Analiza obrazu** - zajmuje się ekstrakcją cech obiektów wysegmentowanych z obrazów na potrzeby rozpoznawania obrazów
  - **Właściwe rozpoznawanie obrazu** - zajmuje się tworzeniem i weryfikacją reguł, na podstawie których udziela się odpowiedzi na powyższe pytanie oraz stosowaniem tych reguł w konkretnych zagadnieniach praktycznych
2. **Oparta na sztucznej inteligencji** - bazuje na cechach wyznaczonych automatycznie w procesie uczenia

# Podsumowanie metod klasycznych

Klasyczne algorytmy rozpoznawania obrazów zawsze zależą od skomplikowanego przetwarzania obrazu w celu poprawy początkowej jakości obrazu i umożliwienia segmentacji / separacji obiektów.

Jednak najważniejszy jest proces inżynierii cech, który jest kluczowy w klasycznej technice rozpoznawania. Tradycyjne „ręcznie” dobierane cechy i funkcje w dużej mierze opierają się na wiedzy specjalistycznej w dziedzinie. Najczęściej są zaproponowane deweloperom systemu przez specjalistów, którzy przygotowują adnotację do zestawu szkoleniowego.



# Rozpoznawanie obrazów metodami opartymi na głębokich konwolucyjnych sieciach neuronowych

Wymagają nauczenia sieci neuronowej rozwiązywania pewnego zadania stosując algorytmy głębokiego uczenia (ang. deep learning) należące do dziedziny zwanej sztuczną inteligencją

# Sztuczna inteligencja

Sformułowanie „sztuczna inteligencja” (ang. Artificial Intelligence; AI) jest używana do nazwania takich komputerów/maszyn, które naśladują „funkcje poznawcze”, które ludzie kojarzą z ludzkim umysłem, takie jak „uczenie się” i „rozwiązywanie problemów”.

Powstała jako dyscyplina akademicka w 1955. Termin zaproponował McCarthy (z Uniwersytetu Stanford) na konferencji w Dartmouth

1. inteligencja realizowana w procesie technicznym, a nie naturalnym, biologicznym;
2. dziedzina badań naukowych informatyki i kognitywistyki czerpiąca także z osiągnięć psychologii, neurologii, matematyki i filozofii.

Definicja z 2019 r: „... zdolność systemu (maszyny, komputera dopisek) do prawidłowego interpretowania danych pochodzących z zewnętrznych źródeł, nauki na ich podstawie oraz wykorzystywania tej wiedzy, aby wykonywać określone zadania i osiągać cele poprzez elastyczne dostosowanie.”

Cytat z: Andreas Kaplan; Michael Haenlein (2019) Siri, Siri in my Hand, who's the Fairest in the Land? On the Interpretations, Illustrations and Implications of Artificial Intelligence, Business Horizons, 62(1), 15-25

# Algorytmy sztucznej inteligencji (AI)

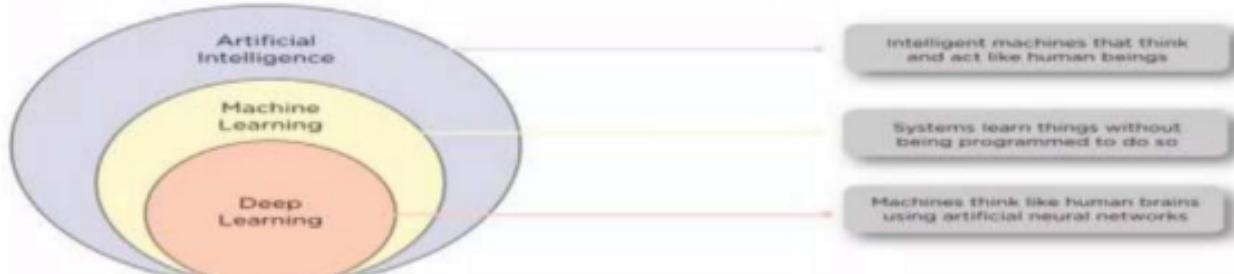
Sztuczna inteligencja jako technologia aktualnie dostępna potrafi:

- Używać naturalnego werbalnego języka, tłumaczyć z języka na język, ale nie potrafi prowadzić komunikacji pozawerbalnej; wyczuć intencji i nastroju mówiącego
- Uczyć się na podstawie danych, na próbach i błędach przez powtarzanie procesy uczenia, ale tylko w stosunku do konkretnego ściśle wyznaczonego zadania
- Otrzymuje bardzo dokładne rezultaty w specyficznych trudnych dla człowieka zadaniach obliczeniowych, w grach o ściśle określonych regułach, poszukiwaniu podobieństwa w danych and nie potrafi żadnej z tych czynności adoptować do nawet lekko zmienionych warunków zadania
- nie ma celu, woli, emocji, poczucia humoru, zawziętości czy wyrozumiałości i innych cech charakteru (indywiduonalności)

Zastosowanie AI w: wizji komputerowej, w rozpoznawaniu mowy, maszynowym tłumaczeniu, w filtrowaniu poczty, graniu w gry nawet trudne jak szachy czy Go . Ostania również odnosi wielkie sukcesy we wspomaganiu diagnostyki w medycynie.

# Uczenie maszynowe czy uczenie się maszyn?

## AI with Machine Learning and Deep Learning



- **Uczenie z nauczycielem, nadzorowane** (supervised learning) – na podstawie przeszłych danych o wejściu i wyjściu dostarczonych przez dewelopera systemu (np. od ekspertów)
- **Uczenie bez nauczyciela, nienadzorowane** (unsupervised learning) – ukryte zależności i organizacja danych, ich podobieństwa i zaburzenia, czy odchylenia od normy są identyfikowane przez system bez pomocy ekspertów w dziedzinie lub dewelopera systemu
- **Nie ma treningu tylko następuje uczenie się dzięki próbom i błędom** (reinforcement learning) i naturalnej pochodzącej ze środowiska karze, która pozwala podnieść efektywność uczenia się np.: uczenie chodu i gry np.: szachy
- **Uczenie częściowo nadzorowane** (weakly supervised), w którym na wstępie zastosowane jest uczenie z nauczycielem na tzn. danych etykietowanych, a następnie zasadnicza część uczenia to uczenie bez nauczyciela.

# Przykłady możliwości systemów opartych na uczeniu maszynowym

- Prowadzenie samochodów i pilotowanie samolotów oraz robotów
- Rozpoznawanie mowy (2012);
- Ekstrahuje i aplikuje cechy stylu  
(Deep Convolution Generative Adversarial Networks DCGAN )



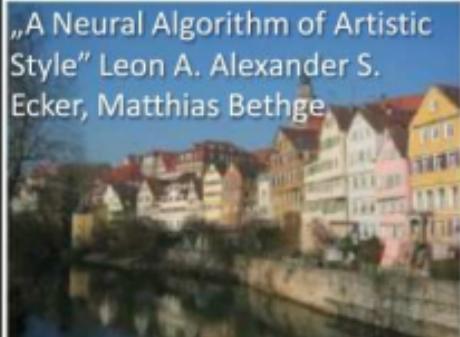
Nvidia

<https://www.youtube.com/watch?v=qhUvQiKec2U>



Boston

Dynamics:  
<https://www.youtube.com/watch?v=e9QzlkP5ql>



„A Neural Algorithm of Artistic Style” Leon A. Alexander S. Ecker, Matthias Bethge



Van Gogh

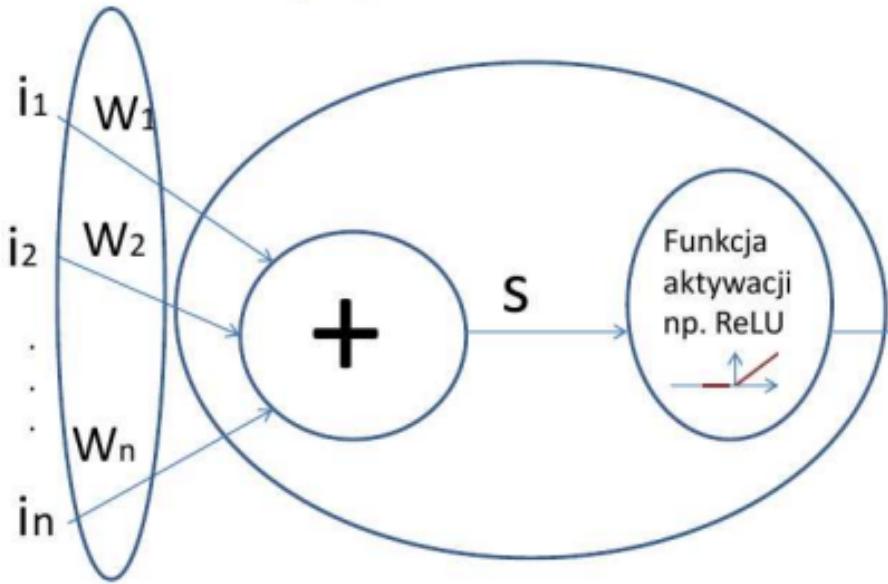


Munch

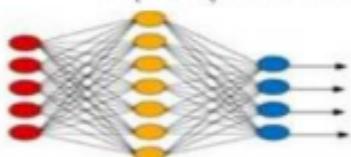


# Jak są zbudowane sztuczne sieci neuronowe?

# Sieci neurunowe



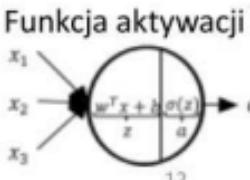
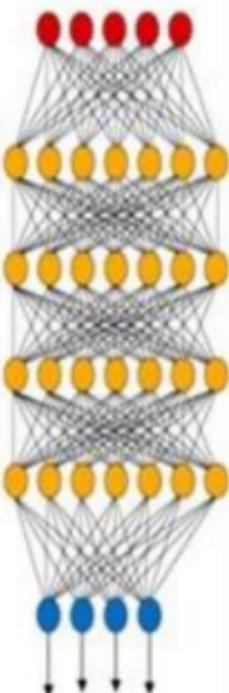
Elementem funkcjonalnym sieci neuronowej jest perceptron / neuron - matematyczna symulacja funkcji komórek nerwowych (odbiór i odesłanie przetworzonego sygnału). Sieć jest złożona z warstw neuronów połączonych w taki sposób, że wyjście warstwy wcześniejszej jest wejściem warstwy następującej po niej. Połączenia poszczególnych neuronów regulują przekazywany sygnał według dobieranych w procesie uczenia współczynników  $W$



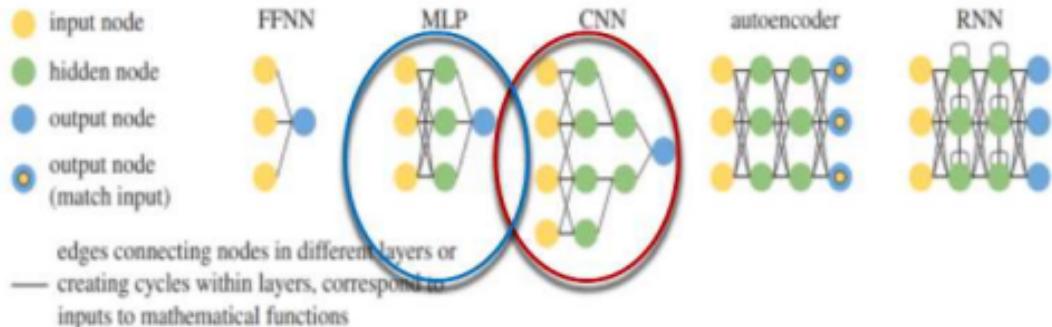
McCulloch and Walter Pitts  
w 1943 roku

# Głębokie sieci neuronowe

- Głębokie sieci neuronowe (NN) to sieci o więcej niż trzech warstwach.
- Sieci neuronowe uczą się z danych źródłowych i mapują „informacje/wiedze wciągniętą ze zbioru uczącego” do **współczynników sieci**.
- W zadaniach rozpoznawania sieci neuronowe potrafią w procesie optymalizacji automatycznie dobrać cechy konieczne do rozpoznawania pewnych klas obiektów w procesie treningu.
- Typowe sieci neuronowe w eksploatacji zachowują się jak „czarna skrzynka”.
- Sieci, w których mamy dostęp do informacji o „przyczynach” decyzji o rozpoznawaniu i klasyfikacji nazywają się po angielski **eXplanable NN; (XNN)**
- Okazuje się, że kombinacja cech pochodzących od ekspertów (używanych w klasycznych metodach rozpoznawania) z cechami zidentyfikowanymi na etapie uczenia się maszyny daje szansę nie tyle bardzo dobre wyniki, ale zrozumiałe dla użytkownika wyniki.



# Sztuczne sieci neuronowe



**Figure 1.** Neural networks come in many different forms. Left: A key for the various types of nodes used in neural networks. Simple FFNN: a feed-forward neural network in which inputs are connected via some function to an output node and the model is trained to produce some output for a set of inputs. MLP: the multi-layer perceptron is a feed-forward neural network in which there is at least one hidden layer between the input and output nodes. CNN: the convolutional neural network is a feed-forward neural network in which the inputs are grouped spatially into hidden nodes. In the case of this example, each input node is only connected to hidden nodes alongside their neighbouring input node. Autoencoder: a type of MLP in which the neural network is trained to produce an output that matches the input to the network. RNN: a deep recurrent neural network is used to allow the neural network to retain memory over time or sequential inputs. This figure was inspired by the Neural Network Zoo by Fjodor Van Veen.

**Headline review**



**Cite this article:** Ching T et al. 2018

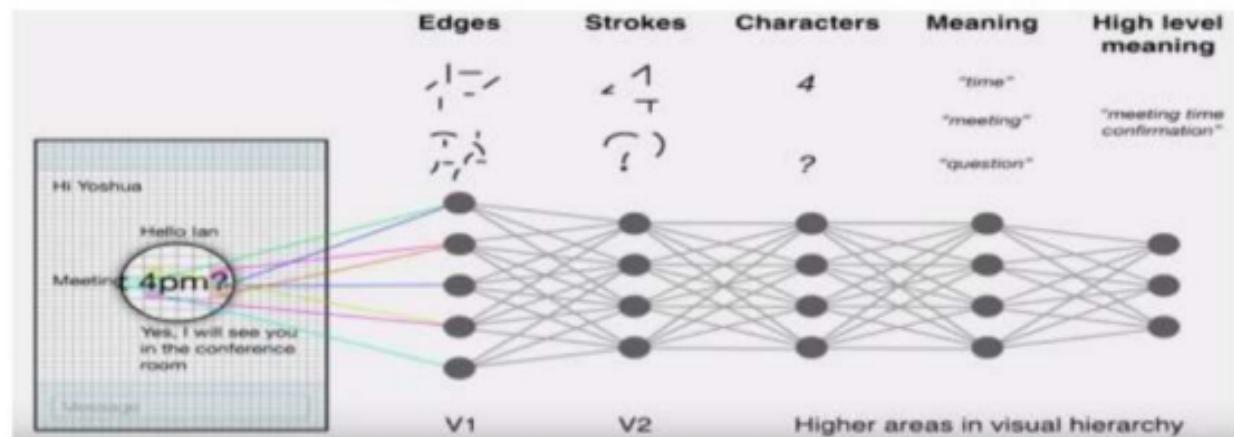
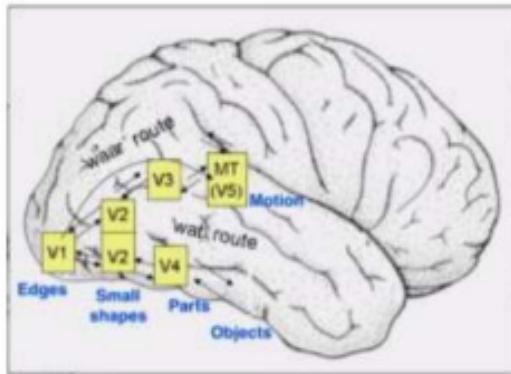
Opportunities and obstacles for deep learning

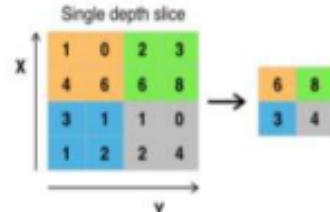
in biology and medicine. *J. R. Soc. Interface* **15**:

20170387.

<https://doi.org/10.1098/rsif.2017.0387>

# Praca głębokiej konwolucyjnej sieci (CNN) imituje proces rozpoznawanie w ludzkim mózgu





# Warstwy

## Podstawowe rodzaje warstw i procesów z nimi związanych:

- **Klasyczna** – Fully Connected (FC) - dense
- **Konwolucyjna** - W odróżnieniu od warstwy typu fully-connected, rozmiar wyniku działania warstwy konwolucyjnej zależy od rozmiaru danych wejściowych, rozmiaru filtrów i funkcji zmieniającej rozmiar, oraz wartości kroku. Sieci tego typu dobrze działają tam gdzie jest duża redundancja informacji np.: przy analizie obrazów, dźwięków lub zbioru cech.
- **Pooling**. Pooling to proces zmniejszeniu przestrzeni cech/rozmiaru sieci wewnętrz konwolucyjnej sieci neuronowej przez uśrednianie (average pooling) lub przyjmowanie wartości maksymalnej (max pooling) z określonego otoczenia.
- **Padding**, czyli uzupełnianie odpowiednimi wartościami, do określonego rozmiaru. Od liczby dodanych zer (stosowany zero padding) zależy, czy mapa wyjściowa będzie miała rozmiar większy, mniejszy czy taki sam, w porównaniu do rozmiaru mapy wejściowej na danym poziomie-warstwie.

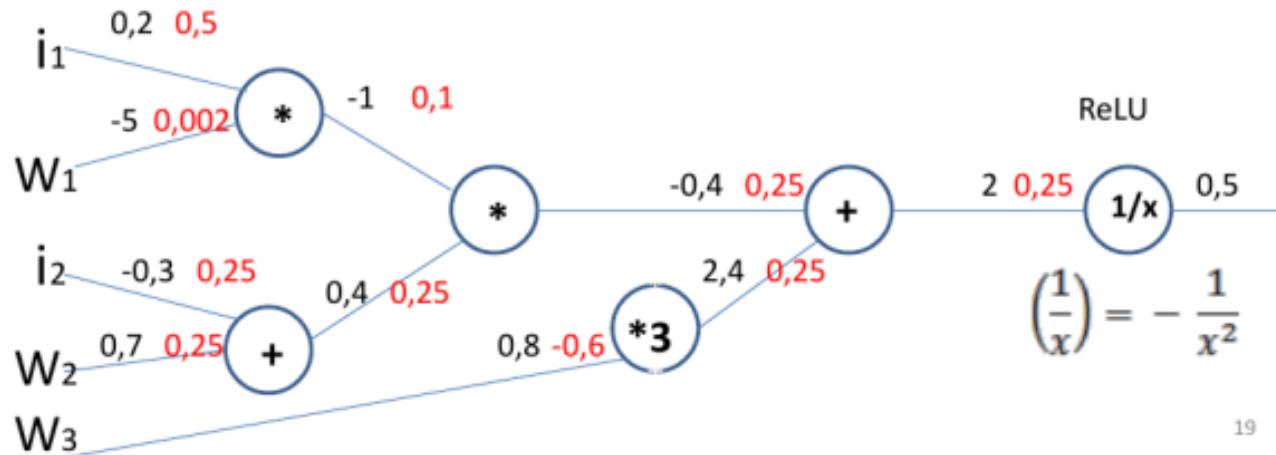
**Jakie matematyczne operacje  
umożliwiają uczenie się sieci**

# Funkcje aktywacji

Name	Plot	Equation	Derivative
Identity		$f(x) = x$	$f'(x) = 1$
Binary step		$f(x) = \begin{cases} 0 & \text{for } x < 0 \\ 1 & \text{for } x \geq 0 \end{cases}$	$f'(x) = \begin{cases} 0 & \text{for } x \neq 0 \\ ? & \text{for } x = 0 \end{cases}$
Logistic (a.k.a Soft step)		$f(x) = \frac{1}{1 + e^{-x}}$	$f'(x) = f(x)(1 - f(x))$
Tanh		$f(x) = \tanh(x) = \frac{2}{1 + e^{-2x}} - 1$	$f'(x) = 1 - f(x)^2$
Arctan		$f(x) = \tan^{-1}(x)$	$f'(x) = \frac{1}{x^2 + 1}$
Rectified Linear Unit (ReLU)		$f(x) = \begin{cases} 0 & \text{for } x < 0 \\ x & \text{for } x \geq 0 \end{cases}$	$f'(x) = \begin{cases} 0 & \text{for } x < 0 \\ 1 & \text{for } x \geq 0 \end{cases}$
Parametric Rectified Linear Unit (PReLU) [2]		$f(x) = \begin{cases} \alpha x & \text{for } x < 0 \\ x & \text{for } x \geq 0 \end{cases}$	$f'(x) = \begin{cases} \alpha & \text{for } x < 0 \\ 1 & \text{for } x \geq 0 \end{cases}$
Exponential Linear Unit (ELU) [3]		$f(x) = \begin{cases} \alpha(e^x - 1) & \text{for } x < 0 \\ x & \text{for } x \geq 0 \end{cases}$	$f'(x) = \begin{cases} f(x) + \alpha & \text{for } x < 0 \\ 1 & \text{for } x \geq 0 \end{cases}$
SoftPlus		$f(x) = \log_e(1 + e^x)$	$f'(x) = \frac{1}{1 + e^{-x}}$

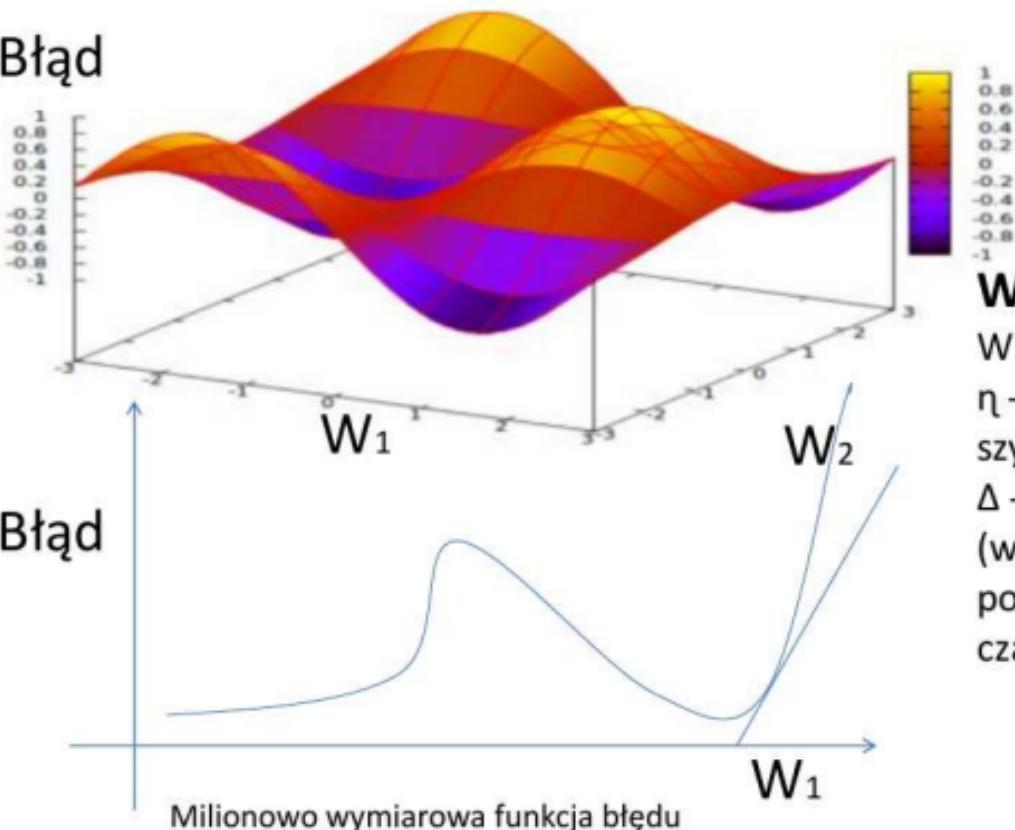
# Algorytm propagacji wstecznej ang. back propagation algorithm

Algorytm oblicza wielkość korekty wag połączeń neuronów rozmieszczonych w sąsiednich warstwach sieci. Oparty jest on na minimalizacji funkcji błędu (np.: sumy kwadratów błędów) uczenia z wykorzystaniem optymalizacyjnej metody największego spadku.



# Funkcja błędu

Błąd



$$W_n = W_p - \eta \Delta$$

$W$  – wektor of  
 $\eta$  - współczynnik  
szybkości uczenia  
 $\Delta$  - gradient  
(wektor  
pochodnych  
częstkowych)

# Pojęcia związane z uczeniem sieci neuronowych

- **Przeuczenia (ang. Overfitting)**: zbyt mała ilość danych w porównaniu do liczby parametrów (zanikanie), zwiększenie zbioru uczącego, zmniejszenie liczby parametrów, losowe wykluczanie neuronów
- **Zanikanie gradientu (ang. Gradients disappears)** zamieniając funkcję aktywacji lub wzmacniając gradient przez regularyzację
- **Zbieżność/konwergencja procesu uczenia (ang. Convergence of learning)** zbieżność procesu optymalizacji zmiana funkcji błędu
- **Ocena poprawności uczenia (ang. Correctness assessment)**: dokładność i precyza, Classical MSE / mutual entropy (CE -cross entropy; Averaged CE (ACE- averaged CE); F1
- **Generalizacja (ang. Generalization)** – cel uczenia

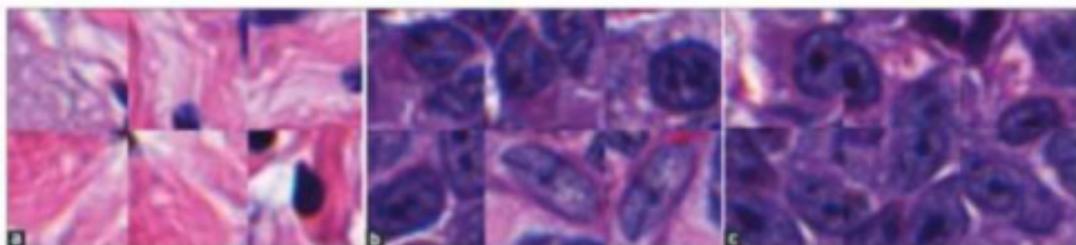
# Augmentacja (ang. augmentation)

To proces powielenia danych uczących przez:

- **Transformacje obrazów** (ang. adversarial transformation); translacje, obroty, przekształcenia afiniczne?
- **Dołożenia pewnych zakłóceń** – rozjaśnienie, przyciemnienia, dodanie szumu zmiana tonacji, itp

J Pathol Inform 2016; 1:29

<http://www.jpathinformatics.org/content/7/1/29>



## **Podsumowanie o sieciach CNN**

# Sztuczna sieć neuronowa

- Poprawa efektywności rozpoznawania, klasyfikacji i segmentacji obrazów przez żmudny **proces optymalizacji sieci – uczenia się**, który przypomina proces Darwinowskiego doboru naturalnego
- Na etapie korzystanie z nauczonej sieci mamy na **wejściu dane, a na wyjściu prawdopodobieństwo** że obiekt należy do którejś ze znanych kategorii **i tylko tyle!**
- **Nie ma „rozumienia”**, bo nie ma kontekstu; nie można wyobrazić sobie konsekwencji, itp.





# CNN wady i zalety

Możliwości CNN:

- Nadzorowane podejście do uczenia maszynowego polega na **szkoleniu modelu statystycznego** przy użyciu zestawu obrazów ze zbioru uczącego, dla których istnieją etykiety i oznaczenia przygotowane przez ekspertów w dziedzinie. Wyuczony model odwzorowuje automatycznie wybrane obiekty na **klasy/kategorie**, czyli uczy się z doświadczeń.
- **Połączenie różnych informacji w modelu** np.: danych klinicznych i obrazów diagnostycznych daje lepsze wyniki predykcji klasyfikacji.



## CNN wady i zalety

CNN mają pewne ograniczenia, które są do pokonania:

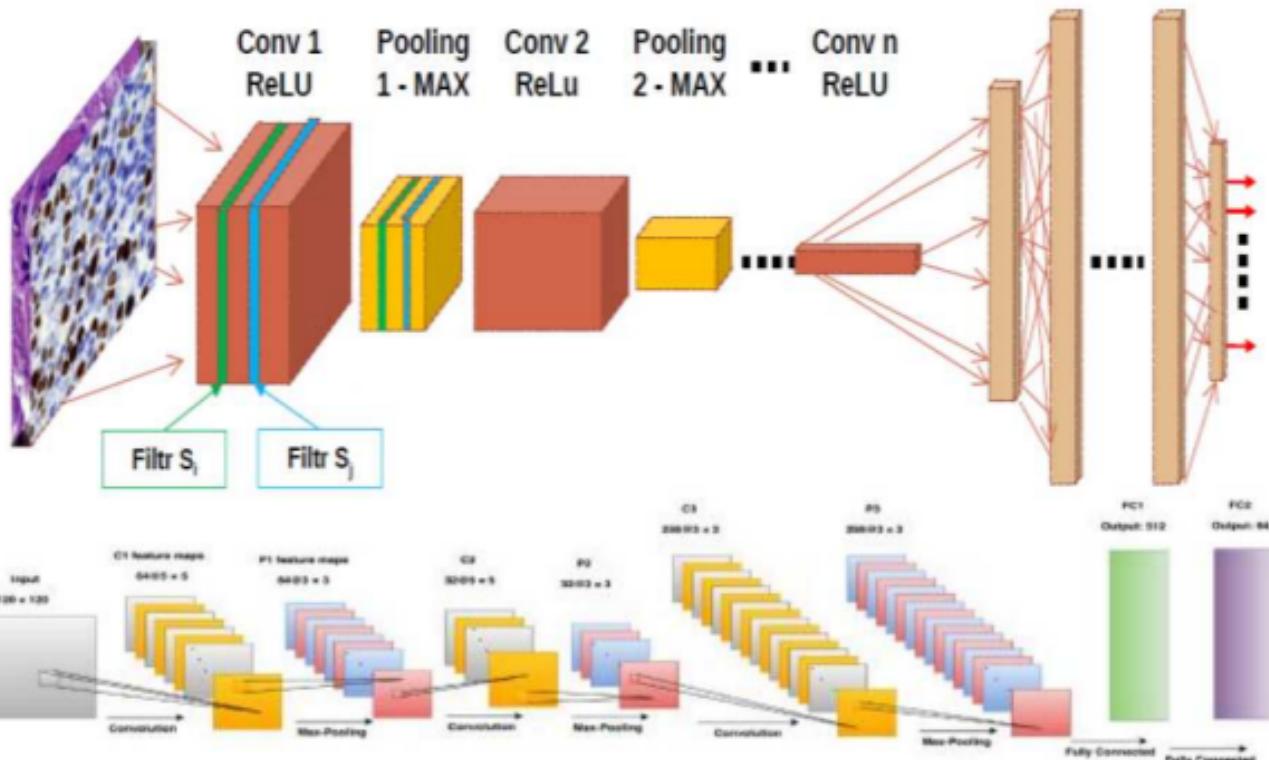
- Uczenie się sieci wymaga ogromnej ilości danych treningowych
- Uczenie się sieci wymaga dużej mocy obliczeniowej
- Proces uczenia się wymagają odpowiedniej architektury wydajnego systemu komputerowego mogą być złożone i często muszą być ścisłe dostosowane do konkretnej aplikacji (programowalne tablice bramek (FPGA), procesory graficzne (GPU) i specyficzne dla aplikacji układy scalone (ASIC)) są badane w celu wykorzystania równoległości struktury obliczeniowej sieci neuronowych, bardziej niż równoległe procesory)
- Powstałe **modele mogą nie być łatwo interpretowalne**
- Długi czas uczenia się (metoda prób i błędów),
- Występowanie nadmiernego dopasowania w przypadku niewystarczającej ilości/liczby danych.
- Trudności w zapewnieniu konwergencji procesu uczenia się.
- **Wymagają od użytkownika zrozumienia, jak należy interpretować wyniki oddawane przez wyuczony model zjawiska/wyuczoną sieć, aby wysunąć sprawdzalne hipotezy dotyczące badań**

## Przykłady sieci

# Sieci, ich autorzy i rok ich powstania

Year	CNN	Developed by	Place	Top-5 error rate	No. of parameters
1998	LeNet(8)	Yann LeCun et al			60 thousand
2012	AlexNet(7)	Alex Krizhevsky, Geoffrey Hinton, Ilya Sutskever	1st		60 million
2013	ZFNet()	Matthew Zeiler and Rob Fergus	1st		
2014	GoogLeNet(19)	Google	1st		4 million
2014	VGG Net(16)	Simonyan, Zisserman	2nd		138 million
2015	ResNet(152)	Kaiming He	1st		

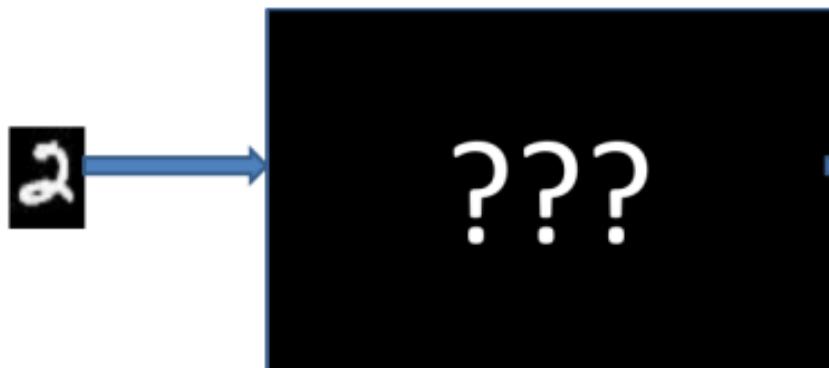
# Podstawowa architektura sieci CNN



# Rozpoznawanie cyfr zapisanych ręcznie

np.: na czekach - Case study

Jak z obrazu uzyskać informację o cyfrze?



$p(\text{obiekt}^{\sim 0})$

$p(\text{obiekt}^{\sim 1})$

$p(\text{obiekt}^{\sim 2})$

$p(\text{obiekt}^{\sim 3})$

$p(\text{obiekt}^{\sim 4})$

$p(\text{obiekt}^{\sim 5})$

$p(\text{obiekt}^{\sim 6})$

$p(\text{obiekt}^{\sim 7})$

$p(\text{obiekt}^{\sim 8})$

$p(\text{obiekt}^{\sim 9})$

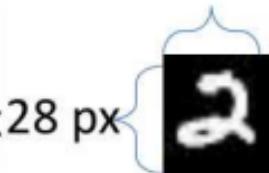
# Baza obrazów MNIST

(Modified National Institute of Standards and Technology)



- 70 000 obrazów ręcznie pisanych cyfr
- 55 000 uczenie, 5 000 walidacja
- 10 000 testy
- 28x28 pikseli
- Wydany w 1998 roku
- 500 różnych osób
- Obraz + etykieta (jaka to cyfra)
- Skala kolorów znormalizowana do 0.0...1.0

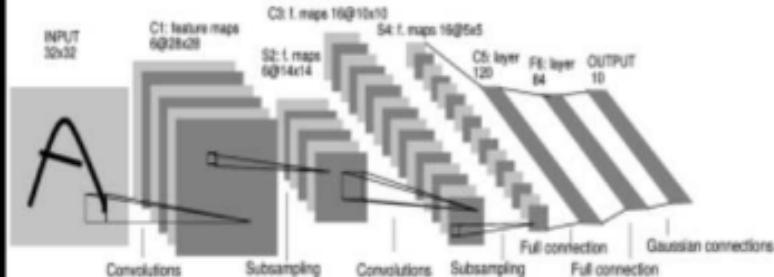
28 px     $28 \times 28 = 784$  pikseli



28 px

Używamy do nauki:  
THE MNIST DATABASE of  
handwritten digits  
<http://yann.lecun.com/exdb/mnist/>

# Sieć LeNet



Model: "sequential\_1"

Layer (type)	Output Shape	Param #
conv2d_2 (Conv2D)	(None, 28, 28, 6)	156
average_pooling2d_2 (AveragePooling2D)	(None, 14, 14, 6)	8
conv2d_3 (Conv2D)	(None, 10, 10, 16)	2416
average_pooling2d_3 (AveragePooling2D)	(None, 5, 5, 16)	8
flatten_1 (Flatten)	(None, 400)	8
dense_3 (Dense)	(None, 120)	48120
dense_4 (Dense)	(None, 84)	10164
dense_5 (Dense)	(None, 10)	850
Total params:	61,706	
Trainable params:	61,706	
Non-trainable params:	0	

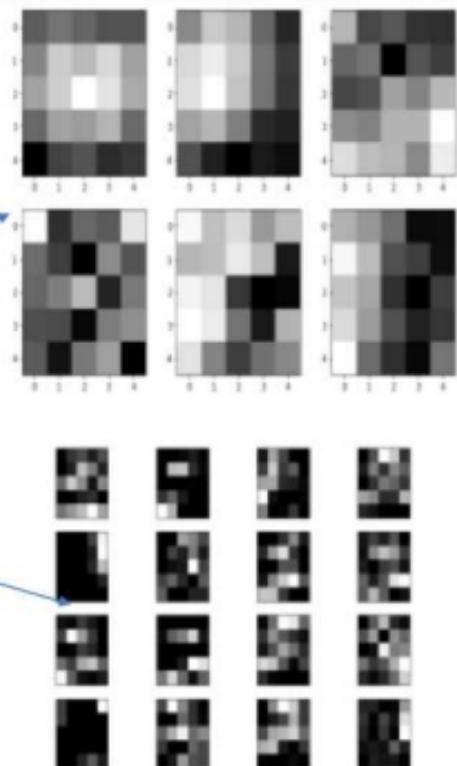
```
37 lenet5 = keras.models.Sequential()
38
39 lenet5.add(keras.layers.Conv2D(filters=6, kernel_size=(5, 5),
40                         activation='relu', input_shape=(32,32,1)))
41 lenet5.add(keras.layers.AveragePooling2D())
42 lenet5.add(keras.layers.Conv2D(filters=16, kernel_size=(5, 5),
43                         activation='relu'))
44 lenet5.add(keras.layers.AveragePooling2D())
45 lenet5.add(keras.layers.Flatten())
46
47 lenet5.add(keras.layers.Dense(units=120, activation='relu'))
48 lenet5.add(keras.layers.Dense(units=84, activation='relu'))
49 lenet5.add(keras.layers.Dense(units=10, activation = 'softmax')) # output
```

Praca zaliczeniowa na APO  
studenta mgr inż. Brylewa

# Uczenie się sieci to optymalizacja ze względu na cel

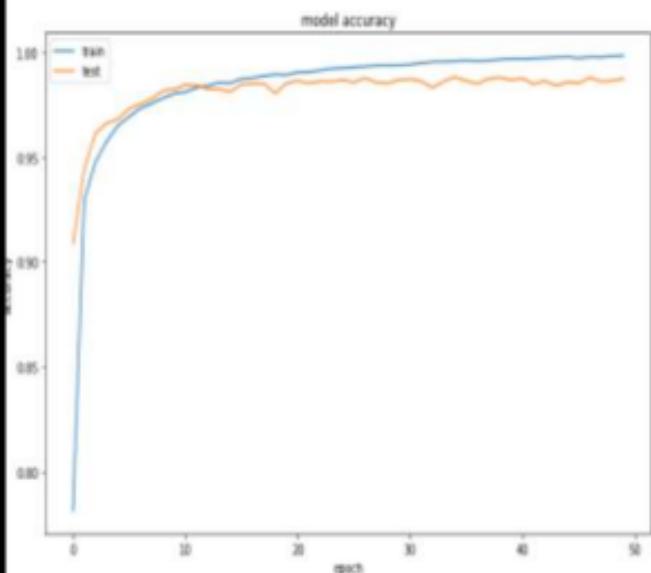
Model: "sequential\_1"

Layer (type)	Output Shape	Param #
conv2d_2 (Conv2D)	(None, 28, 28, 6)	156
average_pooling2d_2 (Average)	(None, 14, 14, 6)	8
conv2d_3 (Conv2D)	(None, 10, 10, 16)	2416
average_pooling2d_3 (Average)	(None, 5, 5, 16)	8
flatten_1 (Flatten)	(None, 400)	0
dense_3 (Dense)	(None, 120)	48120
dense_4 (Dense)	(None, 84)	10164
dense_5 (Dense)	(None, 10)	850
<hr/>		
Total params: 61,706		
Trainable params: 61,706		
Non-trainable params: 0		

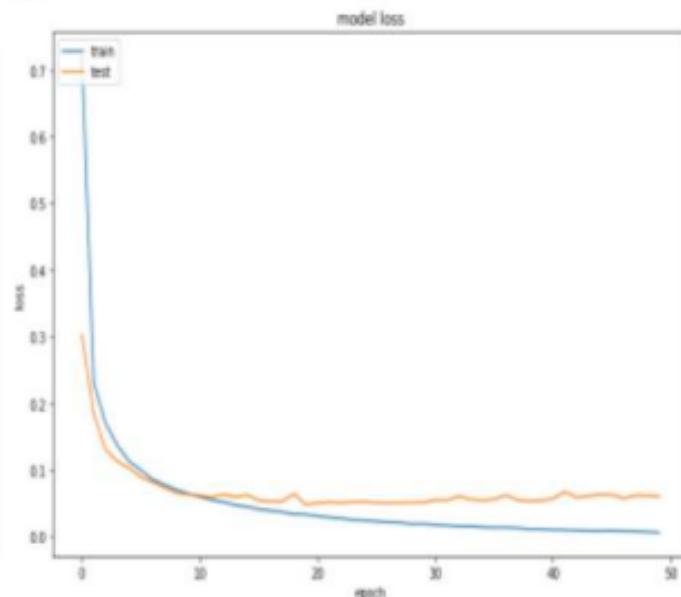


$[-0.0789532 \ -0.02418987 \ 0.10222547 \ 0.00066162 \ -0.04760809 \ 0.09279951 \ -0.01421791 \ -0.07095297 \ 0.05741353 \ -0.01717872]$

# Parametry wyuczenia sieci

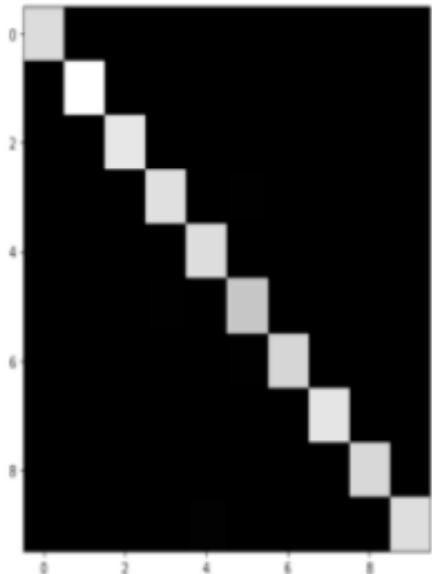


Najlepszego dopasowania



Minimalizacji błędu

# Kontrola błędów



	0	1	2	3	4	5	6	7	8	9
0	[ 974 0 0 0 0 0 2 1 3 0 ]									
1	[ 0 1130 1 0 0 1 2 0 0 1 ]									
2	[ 4 1 1020 0 3 0 0 2 2 0 ]									
3	[ 1 0 2 993 0 6 0 4 2 2 ]									
4	[ 0 0 0 0 976 0 2 2 0 2 ]									
5	[ 2 0 0 7 0 875 2 2 3 1 ]									
6	[ 2 2 0 0 1 5 947 0 1 0 ]									
7	[ 0 3 4 1 1 0 0 1015 2 2 ]									
8	[ 1 0 1 4 3 3 1 2 955 4 ]									
9	[ 2 2 0 4 10 3 0 4 0 984 ]									

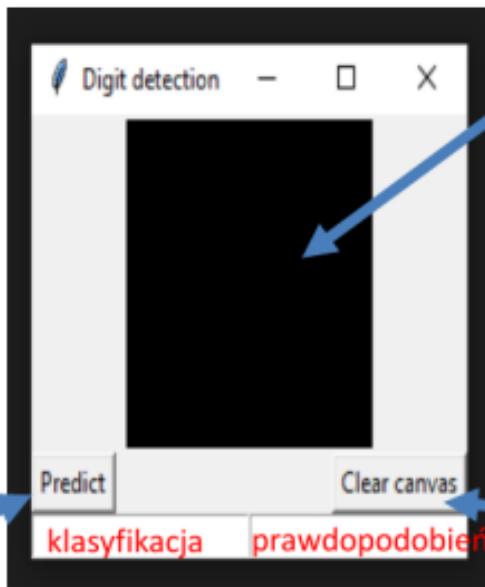
```
result = lenet5.evaluate(X_test, y_test)
dict(zip(lenet5.metrics_names, result))
```

```
313/313 [=====] - 0s 1ms/step - loss: 0.0490 - accuracy: 0.9869
```

```
{'loss': 0.04901135712862015, 'accuracy': 0.9868999719619751}
```

Wizualizacja macierzy pomyłek

# Moduł wykonawczy do rozpoznawania znaków narysowanych przez użytkownika

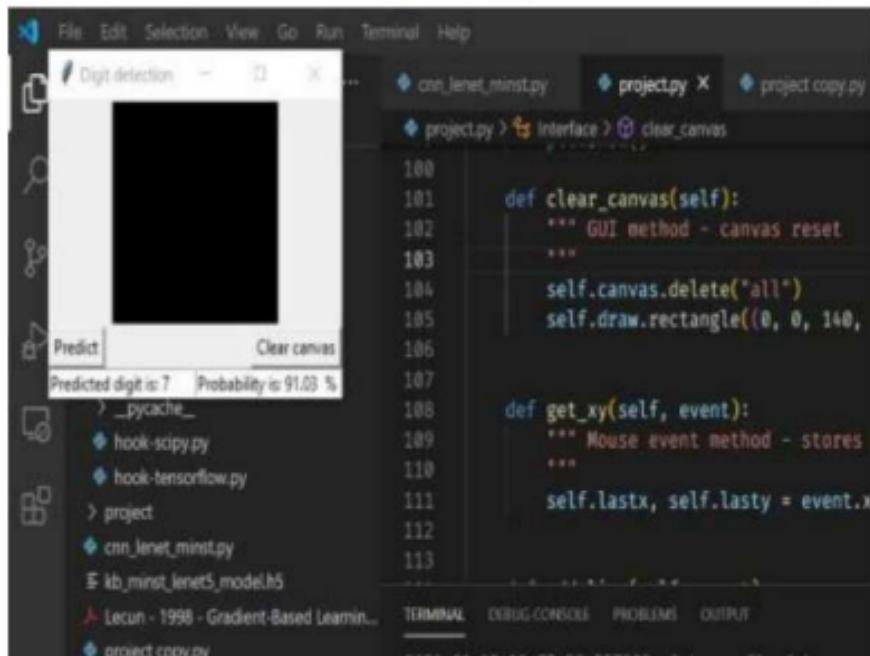


Zamiana obrazu na macierz 32x32 px, wysłanie do modelu, wyliczenia prawdopodobieństw przynależności do jednej z 10 klas i wybór prawdopodobieństwa maksymalnego

Powierzchnia na której można narysować cyfrę do rozpoznania

Czyszczenie powierzchni do rysowania

# Działanie programu rozpoznającego



- Python 3.7
- Numpy
- Matplotlib
- Tensorflow 2.4 – wymaga AVX w zestawie instrukcji CPU!!!
- CUDA 10.1
- SciKit
- Tkinter - GUI

Moduł inferencji

# U-net

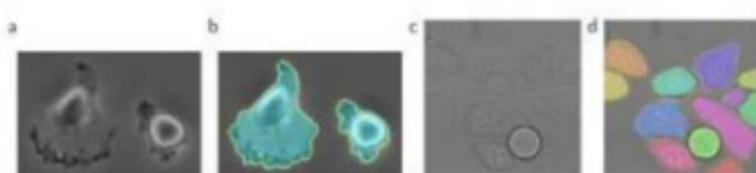
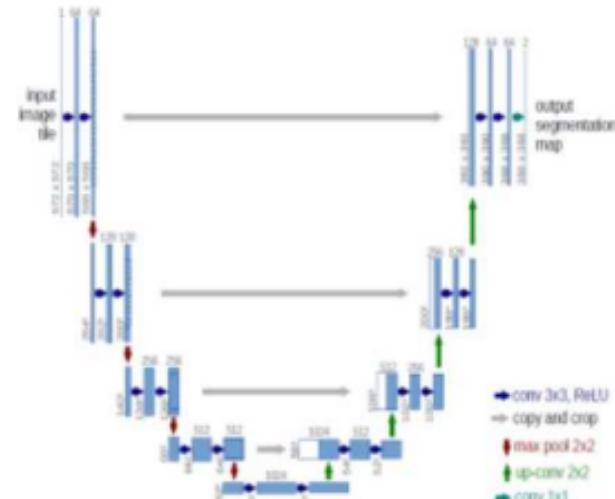
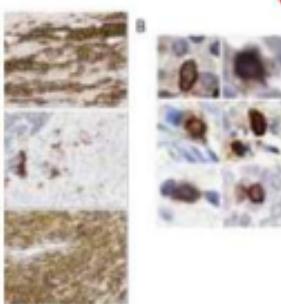
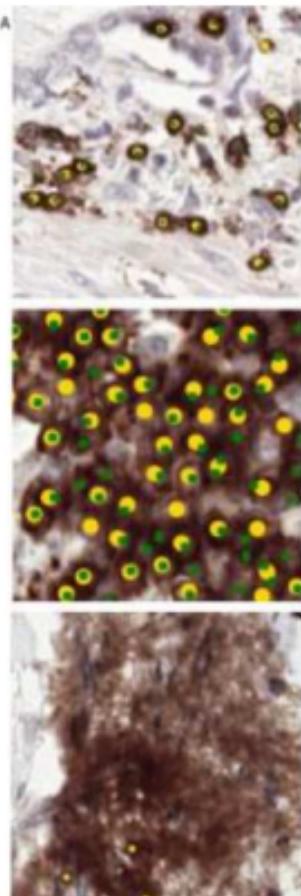
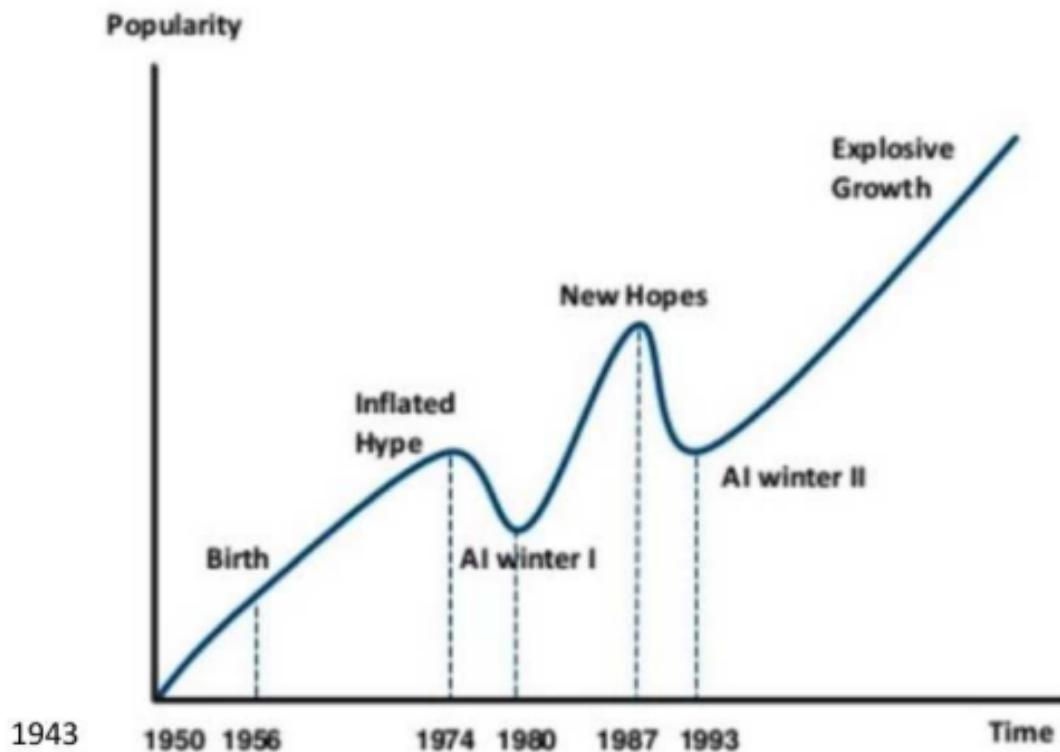


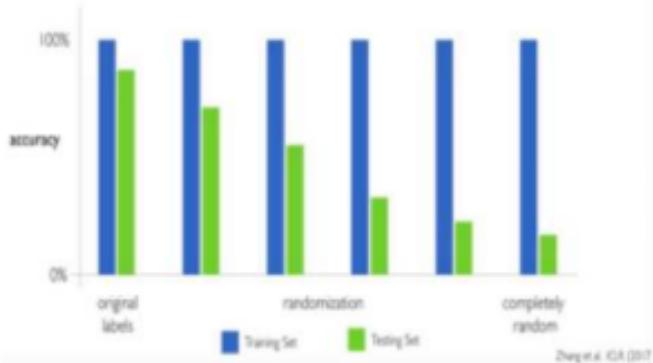
Fig. 4. Result on the ISBI cell tracking challenge. (a) part of an input image of the “PhC-U373” data set. (b) Segmentation result (cyan mask) with manual ground truth (yellow border) (c) input image of the “DIC-HeLa” data set. (d) Segmentation result (random colored masks) with manual ground truth (yellow border).

# **Historia i aktualne problemy NN**



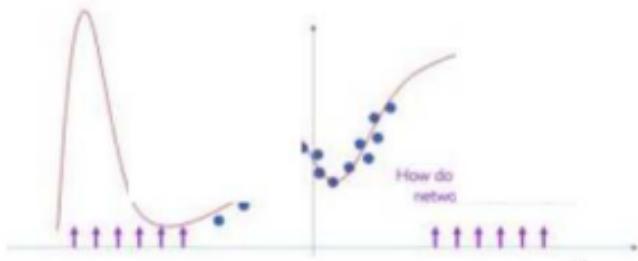
# Ograniczenia DNN

- Można wytrenować sieć, która pasuje do kompletnie przypadkowych podziałów na klasy (na danych treningowych) da 100% dokładności
- Możemy wnioskować o funkcji aproksymującej jedynie w zakresie danych zbioru uczącego.



Zhang et al. ICLR 2017

Neural networks are excellent function approximators  
...when they have training data

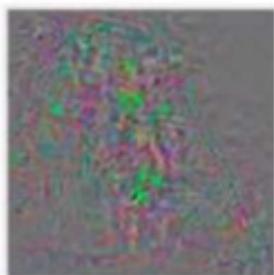


# Ograniczenia DNN

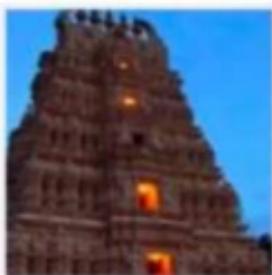
- Uwaga! na proces augmentacji bo czasem produkujemy „podobne przeciwnieństwa” (ang. *adversarial examples*)



Original image  
Temple (97%)



Perturbations



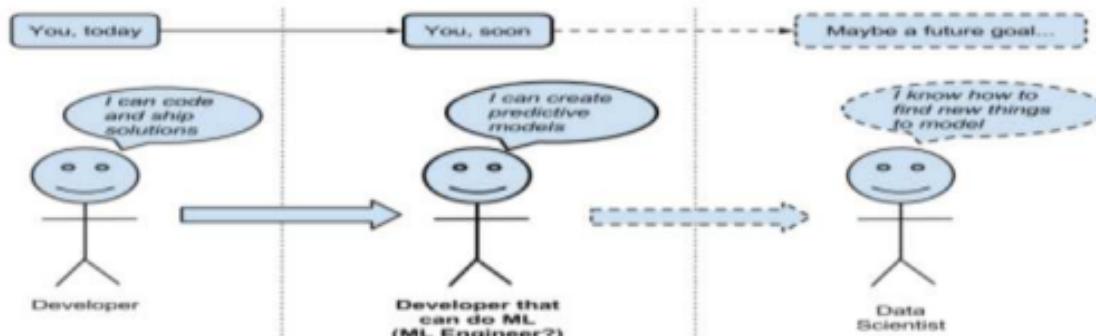
Adversarial example  
Ostrich (98%)

Despois. "Adversarial examples and their implications" (2017).

# Ograniczenia DNN

- Dużo danych bo dużo współczynników do optymalizacji
- Obliczeniowo i wdrożeniowo (GPU) kosztowny
- Mogą być oszukiwane przez „podobne przeciwnieństwa”
- Słabo można zbadać model, jego odporność i niepewność i inne parametry
- Model i oprogramowanie jest **czarną skrzynką** której trudno ufać – **szczególnie ekspertom/lekarzom**
- Nie każde podejście zawsze daje wynik w postaci dobrze optymalizowanej - potrzeba **prób i błędów**
- **Potrzebna wiedza eksperta** (wąskie gardło)

Praca dewelopera oprogramowania w dobie przyszłych mocno zaawansowanych sieci



# Obawy społeczne związane z sztuczna inteligencją

- Przypominają obawy z XIX w sprawie **mechanizacji pracy** lub obawy o Puszkę Pandory
- **Czy technologia może coś chcieć**, być bezwzględnym megalomanem? **Nie ma woli i celu** – to ludzie mają chęć dominacji i gromadzenia zasobów i dokonują projekcji na AI
- Powody nieufności do technologii to głównie: **nieprzejrzystość** i brak dostępu do procesu ich uczenia się sieci (same wyszukują cechy ich zakresy i same się optymalizują wagi, a jak coś idzie nie tak to nadzorujący uczenie się maszyny właściwie nie wiedzą dlaczego, czy to można naprawić. Nadzorujący ponawia proces oparty na przypadkowym podawaniu przykładów ze zbioru uczącego).
- Zbiory uczące przygotowuje **człowiek** i to jego wiedza jest w nich zawarta i przez niego **wyselacjonowana** (postulat: **akredytacje dla deweloperów**).
- Technologia sztucznej inteligencji rozwijana się stopniowo, jest poprawiana pod względem bezpieczeństwa i skuteczności, projektowana, tak aby spełniać różne praktyczne kryteria
- Aktualne sukcesy AI wynikają z ich ogromnej siły obliczeniowej pozwalającej na przeanalizowanie ogromnej ilości danych uczących, czyli przypominanie sawantka czyli genialnego idiota – film „Rainmen” z Dusinem Hofmanem.
- Słowa Alisona Gopinka (University of Clifornia w Berkeley): **„Jak na razie znacznie więcej szkody narobić może naturalna głupota niż sztuczna inteligencja.”**

## Przykłady sieci

# **STEGANOGRAFIA**

# STEGANOGRAFIA

Nauka o komunikacji w taki sposób, by obecność komunikatu nie mogła zostać wykryta, czyli **ukrywanie/hermetyzacji informacji** (ang. *information hiding*)

Słowo „steganografia” pochodzi z języka greckiego i oznacza ukryte pismo

**Zaleta steganografii w stosunku do szyfrowania informacji jest ukrycie samego faktu porozumiewania się stron.**

**Ukrywanie informacji obrazowej (lub tekstowej) w obrazie**  
( *image watermarking* ) w różnych celach:

# Cele stosowania steganografii

1. Ochrona praw autorskich (ukryty obraz (lub tekst) pełni rolę znaku wodnego (*watermark*)), w tym przypadku konieczną własnością obrazu ukrytego jest (poza odpornością na usunięcie przez czynniki zewnętrzne) jego wystarczająca **odporność** na działanie standardowych operacji przetwarzania obrazów (filtracja, kompresja, zniekształcenia geometryczne itp.),
2. Ochrona autentyczności obrazu (ukryty obraz pełni rolę znaku wodnego (*watermark*)), w tym przypadku konieczną własnością obrazu ukrytego jest (poza odpornością na usunięcie przez czynniki zewnętrzne) jego wystarczająca **podatność** na działanie operacji przetwarzania obrazów (filtracja, kompresja, zniekształcenia geometryczne itp.).
3. Praktyczne przesyłania informacji

# Historia steganografii

- Histajos w niewoli króla perskiego Dariusza postanowił przesłać informację do swego zięcia Arystagorasa z Miletu stosując następujący fortel: na wygolonej głowie swego orasa niewolnika **wytatuował informację**, gdy niewolnikowi odrosły włosy posłał go z oficjalnym, mało istotnym listem
- Egipcie i Chinach powszechnie stosowano **atrament sympathyczny**.
- Demaratus ostrzegł Grecję o ataku, pisząc go bezpośrednio na drewnianym podłożu woskowej tabletki przed nałożeniem powierzchni wosku pszczelego.
- **Mikrokropki:** Pierwsze próby miniaturyzowania przesyłanych informacji za pomocą mikrofotografii podjęto w 1871 r. podczas wojny francusko-pruskiej, kiedy to przesyłano raporty do oblężonego przez Niemców Paryża w postaci prostokątów o wymiarach 3 cm × 4 cm. Udoskonalenia tej techniki dokonał wywiad niemiecki Abwehra na początku lat 40. XX wieku.
- punkt o średnicy 1 mm wykonany przez specjalne urządzenie będące połączeniem aparatu fotograficznego i mikroskopu, zawierający zminiaturyzowane dane tekstowe lub fotografie i szczegółowe rysunki techniczne. Skala miniatyrizacji wynosi ok. 1:300, oznacza to możliwość pomniejszenia kartki formatu A4 zawierającej np. tekst do wielkości pojedynczej kropki znajdującej się w tekście pisanej czcionką normalnej wielkości listu.
- Współcześnie technika mikrokropiek (wykonywanych w tysiącach sztuk w technice grawerowania laserowego) jest wykorzystywana także komercyjnie np. do zabezpieczania żetonów w kasynach przed podrabianiem, znakowania samochodów lub cennych przedmiotów.
- **Zapisy kodem pod znaczkiem na liście**
- Podczas II Wojny Światowej Velvalee Dickinson nazywana **Doll Woman** japoński szpieg w Nowym Yorku z lalkami którymi handlowała przesyłała informacje szpiegowskie.
- **Jeremiah Denton** wielokrotnie mrugał oczami w alfabetie Morse'a podczas telewizyjnej konferencji prasowej w 1966 roku, po porwaniu przez porywaczy z Wietnamu Północnego, wypowiadając „T-O-R-T-U-R-E”.
- W 1968 r. członkowie **załogi statku wywiadowczego USS Pueblo**, przetrzymywani przez Koreę Północną jako więźniowie, komunikowali się w języku migowym na zdjęciach.
- Obraz Koranu miał zaszyfrowane informacje o zamachu na World Trade Center

### **Ukrywanie obrazu w obrazie - nazwy obrazów**

1. obraz ukrywający [**p**]
2. obraz ukrywany [**h**]
3. obraz ukrywany po przekształceniu [**hmod**]
4. obraz ukrywający wraz z obrazem ukrytym [**ph**]

### **Obrazy ukrywające z gradacją poziomów szarości**

Obraz ukrywający: na 1 piksel obrazu ukrywanego przypada 1 bajt (8 bitów)

Obraz ukrywany może i powinien być uproszczony: na 1 piksel obrazu może przypadać 1, 2, 3, 4, 5, 6, 7, 8 bitów, co odpowiada 2,4,8,16,32,64,128,256 poziomom szarości (**M**)

W praktyce, ze względu na potrzebę ograniczenia wpływu obrazu ukrywanego na wygląd obrazu ukrywającego, stosowane są wartości **M<<256**, a obraz ukrywany zapisywany jest na najmniej znaczących bitach obrazu ukrywającego.

Zajęcia badanie czy:

przy wzroście wartości **liczby bitów obrazu ukrywanego** następuje coraz większa zmiana wyglądu obrazu ukrywającego i jednocześnie coraz wyraźniejsze uwidocznienie obrazu ukrywanego w tym obrazie.

## **Obrazy ukrywające kolorowe np. w formacie RGB**

Obraz ukrywający: na 1 piksel obrazu przypada 3 bajty (24 bity) odpowiadające 3 składowym R, G, B

Przykładowy zapis piksla obrazu ukrywanego: 2 najmłodsze bity składowej R oraz po jednym najmłodszym bicie składowych G i B (razem 4 bity, co odpowiada obrazowi o  $M=16$  poziomach)

Zapis informacji tekstowej obrazie RGB: 1 znak – 8 bitów co oznacza że do zapisu 1 znaku można wykorzystać 2 piksle.

**Dodatkowe kodowanie obrazów ukrywanych => lepsze ich ukrycie  
(np. przemieszanie poszczególnych piksli)**

**Operacje najczęściej stosowane w procesie ukrywania i odtwarzania obrazu**

- Jednopunktowe jednoargumentowe**

- progowania, redukcji poziomów szarości, rozciągania, uniwersalne operacje punktowe (UOP)

- Jednopunktowe dwuargumentowe**

- arytmetyczne (dodawanie, odejmowanie)
  - logiczne (suma (OR), iloczyn (AND))

**Koniec wykładu**



Egzamin będzie zdalny

# Terminy egzaminu: 02.07.2021 i 09.07.2021

- Egzamin będzie na każdym etapie egzaminem testowym zdalnym.
- Będzie wykonywany przy pomocy oprogramowania **Inspera**.
- Kursy dla studentów na temat tego oprogramowania już się odbyły, ale można je jeszcze raz przejść rozwiązuając udostępnione testy.

↶ ↷ | **B** *I* U  $\times_r$   $\times^2$  |  $\frac{\partial}{\partial x}$   $\frac{\partial^2}{\partial x^2}$  |  $\otimes$   $\otimes^2$  |  $\odot$   $\Sigma$  | % | = |

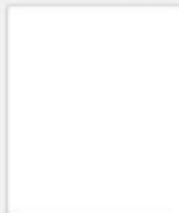
+ Wstaw element

Napisz, co to jest obraz cyfrowy.



- Punkty
- Główna ilustracja
- Panel PDF
- Etykiety

Napisz, co to jest obraz cyfrowy.



Outlook Web App x Tłumacz Google x Inspera Assessment x obraz cyfrowy - Szukaj w Google x +

← → C google.com/search?q=obraz+cyfrowy&rlz=1C1N&XL\_plPL771PL771&oiq=obraz+cyfrowy&oq=chrome\_6957j0l7.5430j08&sourceid=chrome&ie=UTF-8

Aplikacje Chrome Citibank Online - M... Credit Agricole Ban... PRACA & GRANTY... UBBK | Uczelniowy B... Home - Lumosity zdrofit Tłumacz Google

# Google

obraz cyfrowy

X

Wszystko Grafika Zakupy Wiadomości Filmy Więcej Ustawienia Narzędzia

Okolo 47 800 000 wyników (0.56 s)

**Obraz cyfrowy** (ang. digital image) – dwuwymiarowy obraz zapisany w postaci binarnej, możliwy do przechowywania w pamięci cyfrowej. Pojęcie najczęściej dotyczy obrazu zapisanego w postaci rastrowej, w której jest on przedstawiony jako dwuwymiarowa macierz pikseli.

[pt.wikipedia.org › wiki › Obraz\\_cyfrowy](#)

**Obraz cyfrowy – Wikipedia, wolna encyklopedia**

Informacje o fragmentach z odpowiedzią Przeslij opinię

[www.szkolazpasia.pl › rastrowa › istota-obrazu-cyfrowego](#)

**ISTOTA OBRAZU CYFROWEGO - Informatyka Jacek Turlejski**  
ISTOTA OBRAZU CYFROWEGO 3.1. PIKSEL. Obrazy cyfrowe, odzwierciedlające oryginały, noszą także nazwę obrazów bitmapowych, map bitowych lub po ...

[www.zsk.ict.pwr.wroc.pl › zsk › loc › in\\_obi\\_wyk\\_1](#)

**Obraz cyfrowy - Politechnika Wrocławska**  
Jak wyrazić cechy obrazu przy pomocy liczb? • Podstawy przetwarzania obrazów cyfrowych. Jacek Jarnicki Politechnika Wrocławska. 3. 1. Obraz cyfrowy i jego ...

[https://allegro.pl/oferta/120x80-duzy-obraz-cyfrowy-natura-89737630117?utm\\_feed=a34192d-eee2-4419-9a9a-de66b9dfac28](https://allegro.pl/oferta/120x80-duzy-obraz-cyfrowy-natura-89737630117?utm_feed=a34192d-eee2-4419-9a9a-de66b9dfac28)

Zobacz: obraz cyfro...

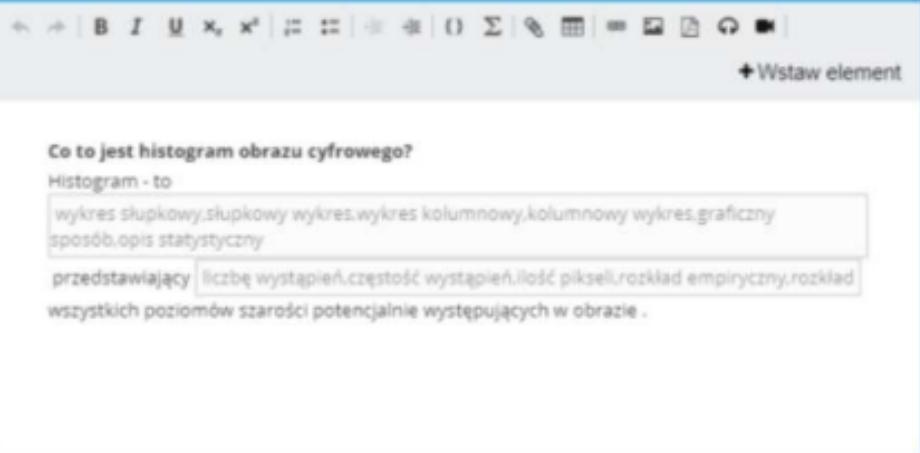
  
Hama Slimline Basic 8" Cyfrowa ramka do zdjęć 229,00 zł RTV Euro AGD Przez: PMshopping

  
Graffiti B... Obraz cy... 194,00 zł artspesaz...

  
T 7" 8" 10" mm/152mm/177mm 120x80 Du... Cudowny Na...



PENNY OPIS EN 0...dock ^ PENNY OPIS EN 0...dock ^



- Punkty
  - Główna ilustracja
  - Panel PDF
  - Etykiety
  - Zaawansowane

## def histogramu

## Co to jest histogram obrazu cyfrowego?

Histogram - to wykres zawierający 256 punktów na poziomej osi, które określają jasność pikseli na zdjęciu.

**x** (wykres słupkowy, słupkowy wykres) przedstawiający w zakresie [0,255]

(liczbe wystąpień, częstość wystąpień) wszystkich poziomów szarości potencjalnie występujących w obrazie.

# Histogram

[edytuj]

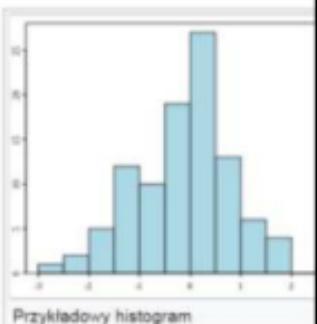
Histogram – jeden z graficznych sposobów przedstawiania rozkładu empirycznego cechy. Składa się z szeregu prostokątów umieszczonych na osi współrzędnych. Prostokąty te są z jednej strony wyznaczone przez przedziały klasowe (patrz: szereg rozdzielczy) wartości cechy, natomiast ich wysokość określona przez liczebności (lub częstotliwości, ewentualnie gęstość prawdopodobieństwa) elementów wpadających do określonego przedziału klasowego.<sup>[1]</sup> Jeśli histogram pokazuje liczebności, a nie gęstość prawdopodobieństwa, wówczas szerokości przedziałów powinny być równe.

## Interpretacja histogramu

[edytuj] [edytuj kod]

Przykładowa interpretacja histogramu z rysunku obok:

- luka w histogramie:
  - podejrzenie nieprawidłowego odczytu (brak danych),
  - podejrzenie błędu urządzenia pomiarowego.
- histogram z dwoma wierzchołkami:
  - tzw. rozkład dwumodalny, który powstaje często, gdy badana populacja jest połączeniem dwóch odseparowanych populacji, np. połączono wyroby z różnych procesów wytwórczych.



Zobacz też [edytuj] [edytuj kod]

sample.wig

PEŁNY OPS EN 0...docx



Pokaż w

← → | B I U ×, ×² | ← → | 0 Σ | ↻ | ← → |

Wstaw element

Na obrazie o M = 6 i N = 4

1	2	3	4
1	0	0	0
0	5	4	1
1	4	3	0
0	0	0	0

wykonaj operację progowania według progu th = 2. Zapisz operację w postaci tablicy LUT:

0	1	2	3	4	5
0,0	0,0	0,0	5,5	5,5	5,5

oraz obraz wynikowy

0,0	0,0	0,0	0,0
0,0	5,5	5,5	0,0
0,0	5,5	5,5	0,0
0,0	0,0	0,0	0,0

## Progowanie

Jest to taka wersja operacji zmniejszenia ilości poziomów szarości do dwóch, dla której istnieje możliwość arbitralnego wyboru wartości progu ( $p_1$ ) czyli szarości granicznej, od której przyporządkowujemy wyższy poziom szarości (najczęściej biały) i poniżej której przyporządkowujemy niższy próg szarości (najczęściej czarny).

$$q = \begin{cases} L_{\min} & \text{dla } p \leq p_1 \\ L_{\max} & \text{dla } p > p_1 \end{cases}$$

Punkty

Główna ilustracja

Panel PDF

Etykiety

Punkty

Główna ilustracja

Panel PDF

Etykiety

Na obrazie o M = 6 i N = 4

1	2	3	4
5	5	4	5
4	0	0	5
4	0	1	5
4	5	5	5

wykonaj operację progowania binarnego z progiem  $th = 3$ . Zapisz operację przy pomocy tablicy LUT:

0	1	2	3	4	5
0,0	0,0	0,0	0,0	1,1	1,1

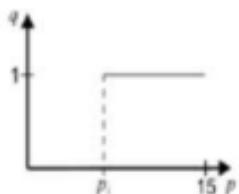
oraz obraz wynikowy:

5,5	5,5	5,5	5,5
5,5	0,0	0,0	5,5
5,5	0,0	0,0	5,5
5,5	5,5	5,5	5,5

### Operacja progowania (binaryzacji)

$$p_1 = 5$$

$$q = \begin{cases} 0 & \text{dla } p \leq p_1 \\ 1 & \text{dla } p > p_1 \end{cases}$$



15	15	0	0	2
13	13	15	0	0
0	0	7	14	14
0	1	2	3	4
15	14	13	12	11

1	1	0	0	0
1	1	1	0	0
0	0	1	1	1
0	0	0	0	0
1	1	1	1	1

[Punkty](#)
[Główna ilustracja](#)
[Panel PDF](#)
[Etykiety](#)

Na obrazie o  $M = 6$  i  $N = 4$

1	2	3	4
1	0	0	2
0	5	4	1
1	4	3	0
0	0	0	0

wykonaj operację progowania odwrotnego z progiem  $th = 2$ . Zapisz tę operację w postaci tablicy LUT:

0	1	2	3	4	5
5.5	5.5	5.5	0.0	0.0	0.0

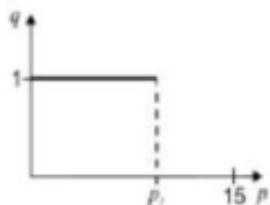
oraz obraz wynikowy

5.5	5.5	5.5	5.5
5.5	0.0	0.0	5.5
5.5	0.0	0.0	5.5
5.5	5.5	5.5	5.5

### Operacja odwrotnego progowania (binaryzacji)

$$p_1 = 5$$

$$q = \begin{cases} 1 \text{ dla } p \leq p_1 \\ 0 \text{ dla } p > p_1 \end{cases}$$



15	15	0	0	2
13	13	15	0	0
0	0	7	14	14
0	1	2	3	4
15	14	13	12	11

0	0	1	1	1
0	0	0	1	1
1	1	0	0	0
1	1	1	1	1
0	0	0	0	0

# Jak rozwiązywać zadania obliczeniowe?

- Zadania z liczeniem odległości

## Metryka Euklidesowa

$$\rho_1(\underline{x}^\mu, \underline{x}^\eta) = \sqrt{\sum_{v=1}^n (x_v^\mu - x_v^\eta)^2}$$



## Metryka uliczna (Manhattan, city block distance):

$$\rho_2(\underline{x}^\mu, \underline{x}^\eta) = \sum_{v=1}^n |x_v^\mu - x_v^\eta|$$

## Metryka Czebyszewa (maksymalna)

$$\rho_3(\underline{x}^\mu, \underline{x}^\eta) = \max_{1 \leq v \leq n} |x_v^\mu - x_v^\eta|$$

# Jak rozwiązywać zadania problemowe?



- Czym różni się akwizycja w przypadku tych trzech obrazów dloni?
- Czym różni się zapis informacji o obrazie dla tych trzech obrazów dloni?



**Życzę powodzenia na egzaminie**





