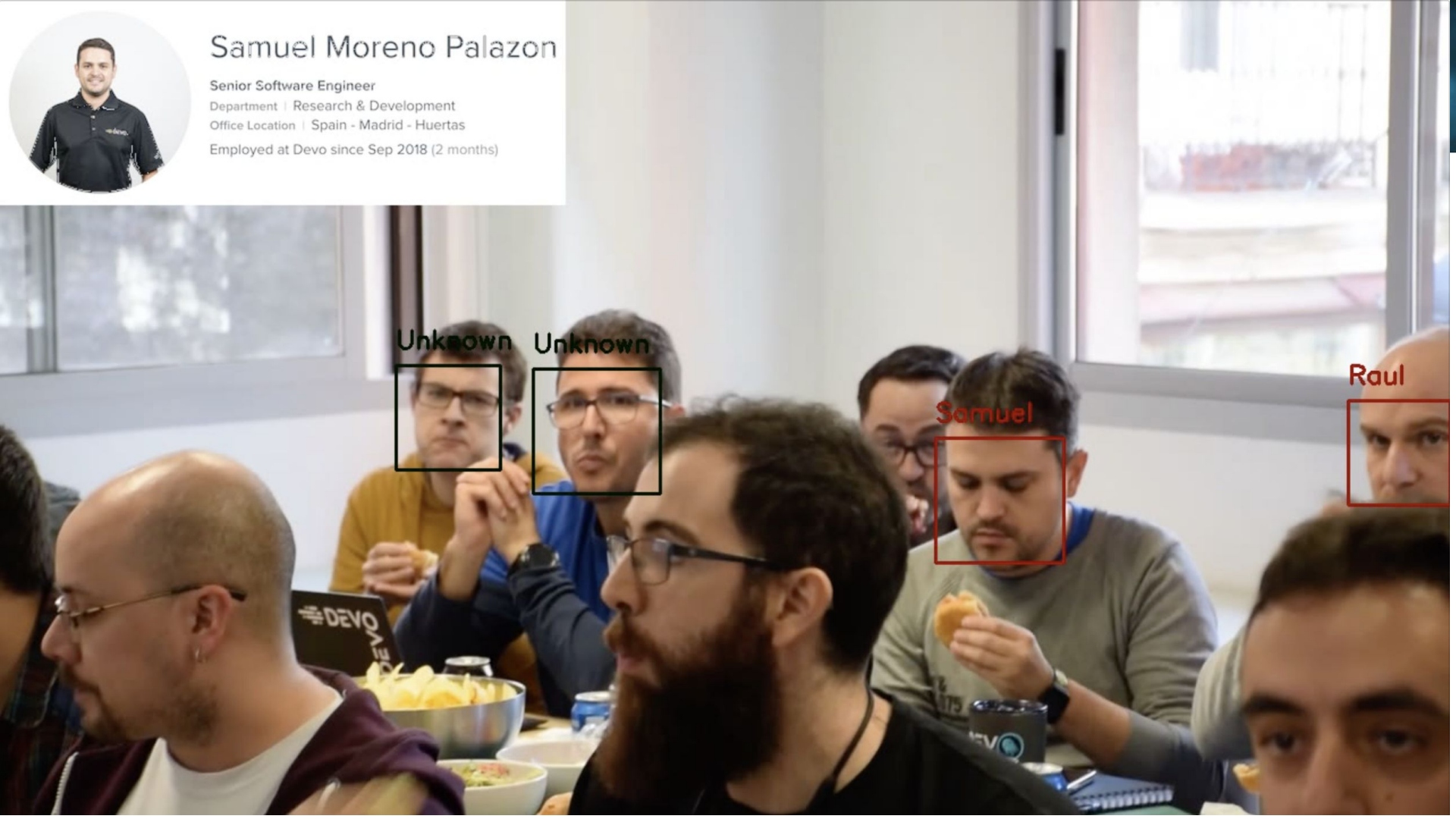

black hat
EUROPE 2018
DECEMBER 3-6, 2018
EXCEL LONDON / UNITED KINGDOM
Video Killed the Text Star:
OSINT Approach
#BHEU / @BLACK HAT EVENTS

Fran Gomez
@ffranz

Cesar Jimenez
@cesarjz

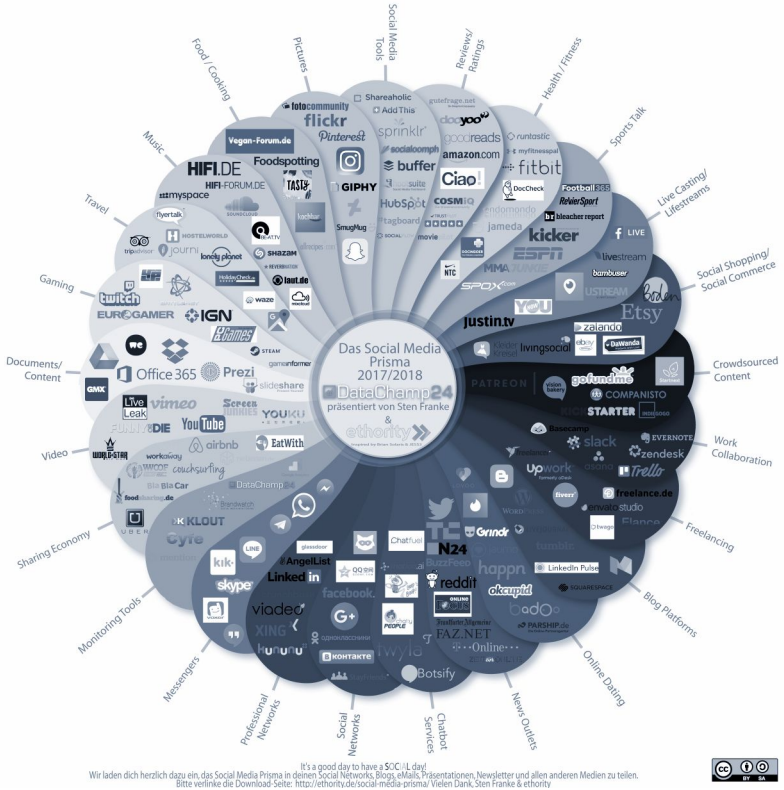
DEVO


Samuel Moreno Palazon
Senior Software Engineer
Department | Research & Development
Office Location | Spain - Madrid - Huertas
Employed at Devo since Sep 2018 (2 months)
Unknown
Unknown
Samuel
Raul
DEVO

1. OSINT
2. Video analysis
3. Faces Recognition
    a. Where are the faces?
    b. Faces encoding
    c. Identify persons
4. Video Demo
5. Architecture
6. Code
7. Identify unknowns
8. Social Impact
9. Defense

OSINT

“Information does not have to be secret to be valuable”



https://ethority.de/social-media-prisma/

OSINT

Open-source intelligence is the data collected from publicly available sources to be used in an intelligence context.

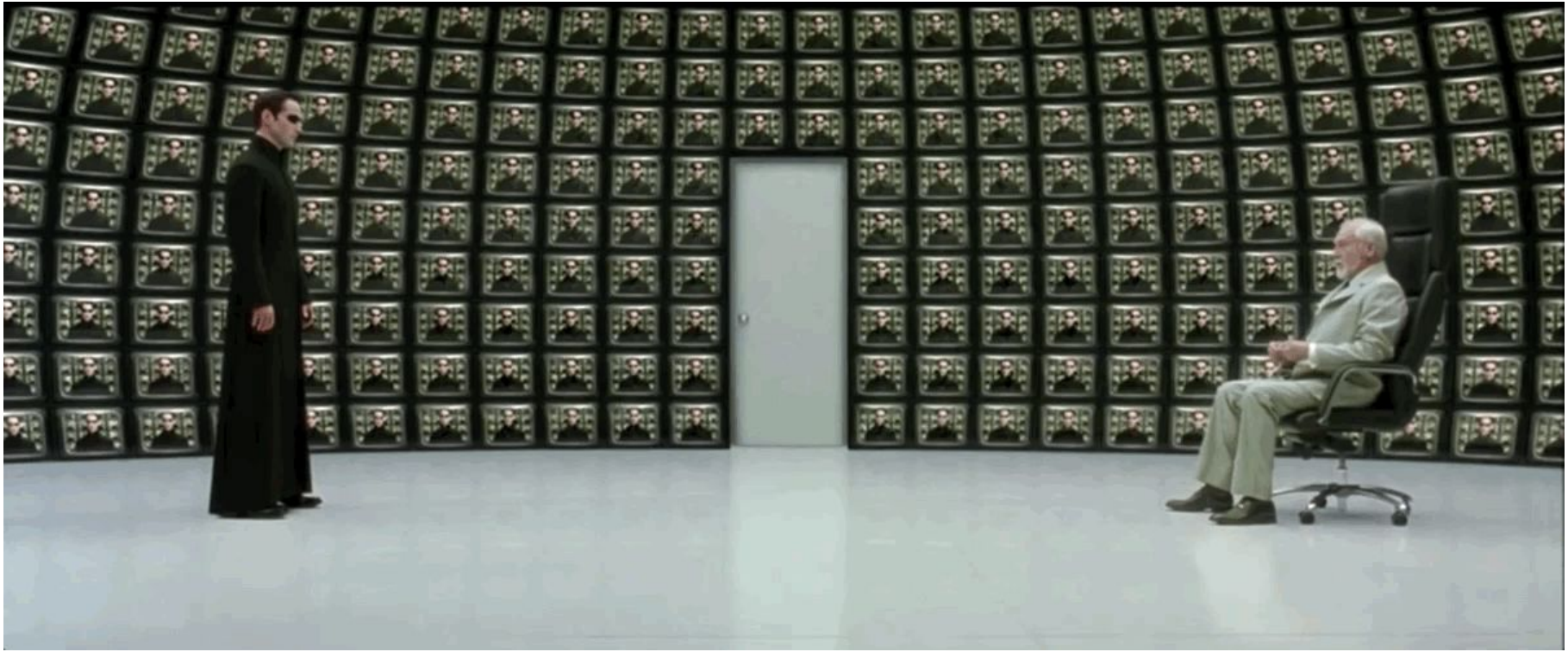
The development of behavior forecasts or recommended courses of action to the leadership of an organisation, based on wide ranges of available overt and covert information.

Wikipedia contributors. (2018, September 23). Open-source intelligence. In Wikipedia, The Free Encyclopedia. Retrieved 18:07, October 19, 2018, from https://en.wikipedia.org/w/index.php?title=Open-source_intelligence&oldid=860809738
Wikipedia contributors. (2018, October 3). Intelligence assessment. In Wikipedia, The Free Encyclopedia. Retrieved 18:07, October 19, 2018, from https://en.wikipedia.org/w/index.php?title=Intelligence_assessment&oldid=862306387

Use Cases

- National Security
- Counterterrorism
- Cyber Tracking of terrorists
- Search missing persons
- Identify persons related to sexual violence crimes
- Identity theft
- Monitor competitors activities
- Gather information about a specific target (Hacking)
- Marketing ROI (Sports, YouTube, …)

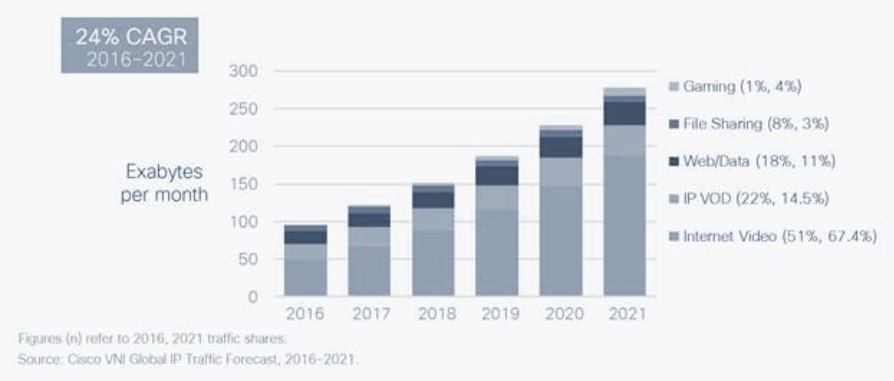
Video Analysis



Video Traffic

By 2021, 80% of the World's Internet Traffic Will Be Video

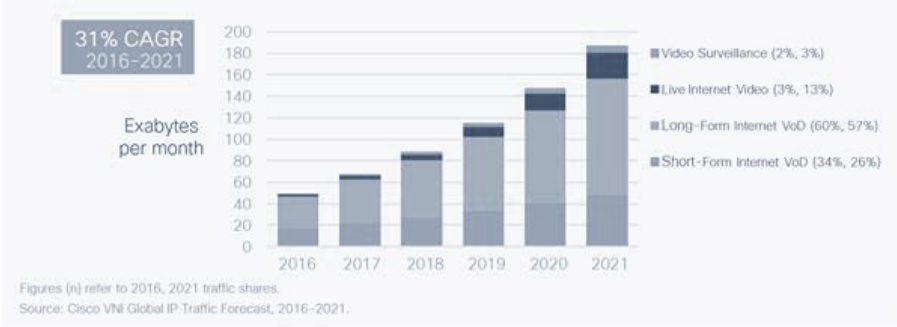
Video Traffic



2018. Video Traffic ~90 Exabytes per month
90 Million Terabytes
90.000.000.000.000.000.000 bytes

2018. Video Surveillance Traffic ~0.18 (2%) Exabytes per month

180.000 Terabytes
180.000.000.000.000.000 bytes



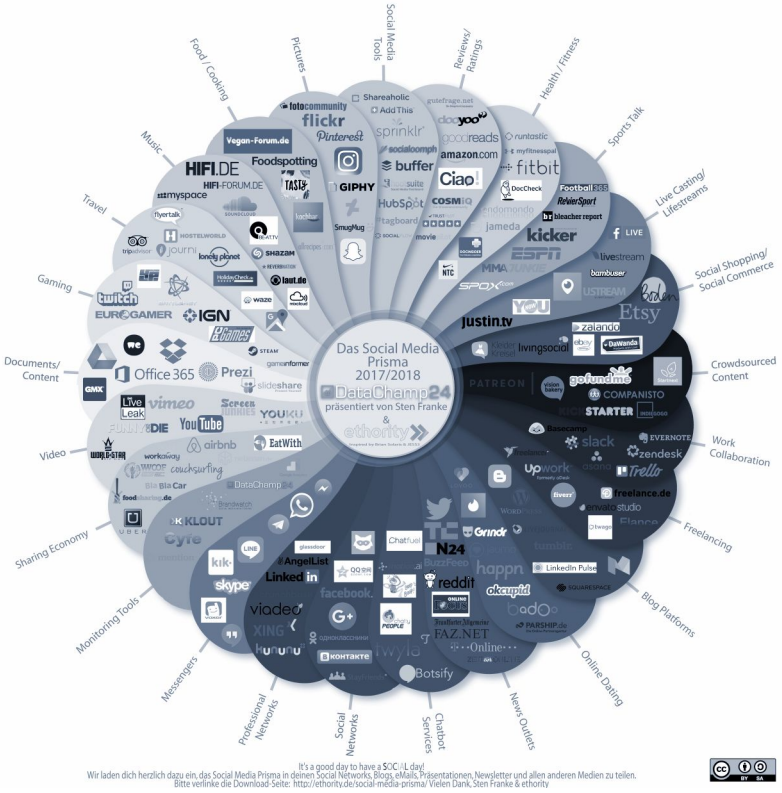
https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

Video Traffic

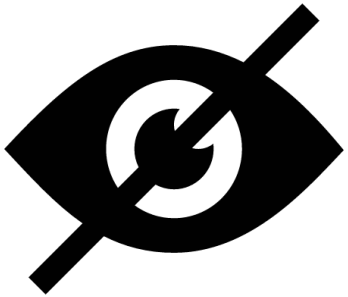
twitch

LIVE

YouTube



https://ethority.de/social-media-prisma/



Sensitive Content

Next content contains sensitive content which some people may find offensive or disturbing

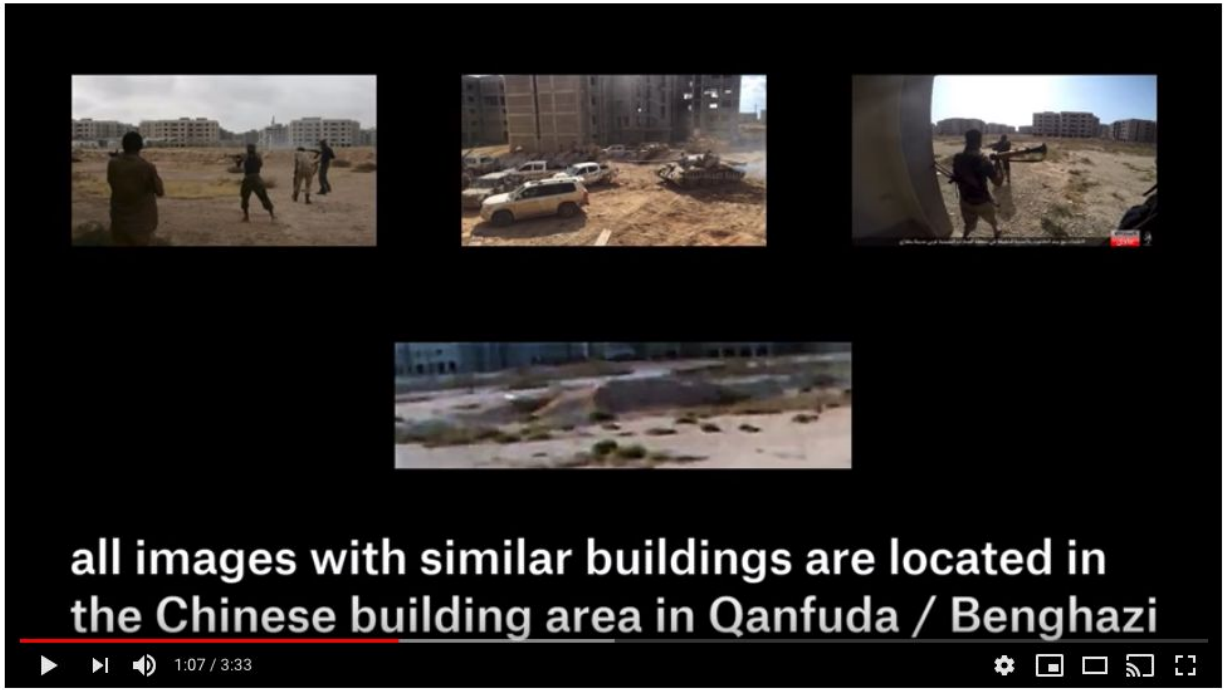
Video Analysis

Where

https://foreignpolicy.com/2018/09/25/google-maps-is-a-better-spy-than-james-bond/amp/?__twitter_impression=true

Video Analysis

Where



https://foreignpolicy.com/2018/09/25/google-maps-is-a-better-spy-than-james-bond/amp/?__twitter_impression=true

Video Analysis

Where

https://foreignpolicy.com/2018/09/25/google-maps-is-a-better-spy-than-james-bond/amp/?__twitter_impression=true

Video Analysis

When

https://foreignpolicy.com/2018/09/25/google-maps-is-a-better-spy-than-james-bond/amp/?__twitter_impression=true

Video Analysis

When

https://foreignpolicy.com/2018/09/25/google-maps-is-a-better-spy-than-james-bond/amp/?__twitter_impression=true

Video Analysis

When

https://foreignpolicy.com/2018/09/25/google-maps-is-a-better-spy-than-james-bond/amp/?__twitter_impression=true

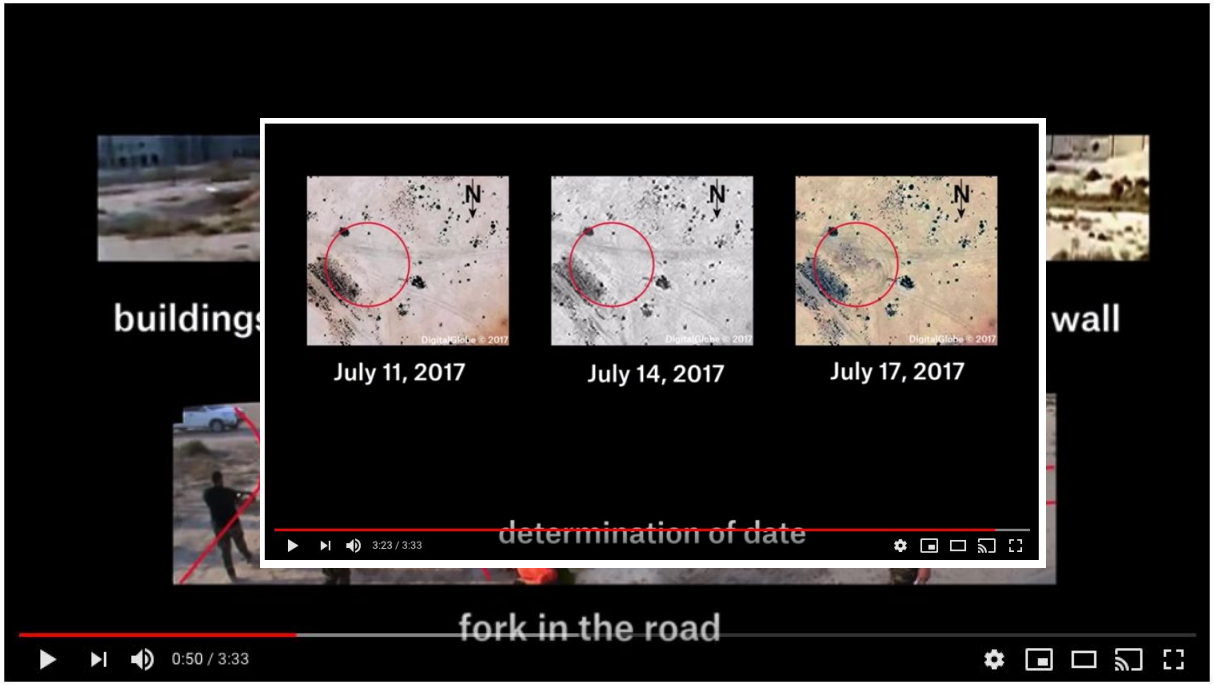
Video Analysis

When

https://foreignpolicy.com/2018/09/25/google-maps-is-a-better-spy-than-james-bond/amp/?__twitter_impression=true

Video Analysis

When

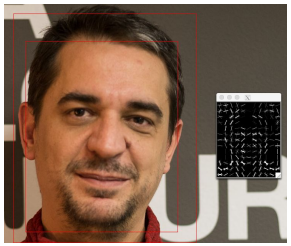


https://foreignpolicy.com/2018/09/25/google-maps-is-a-better-spy-than-james-bond/amp/?__twitter_impression=true

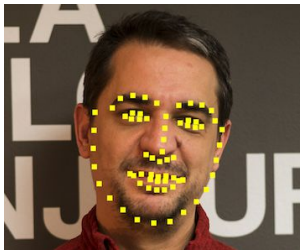
Facial Recognition

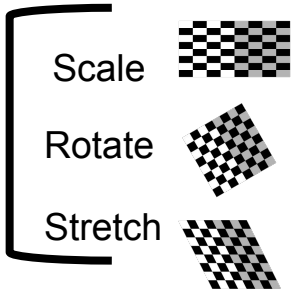
Human face recognition is one of Machine Learning applications which most advanced in recent years.

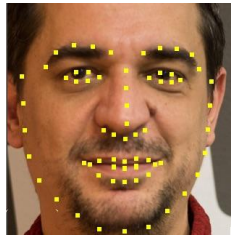
HOG or CNN

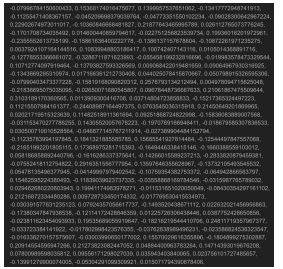


Landmarks

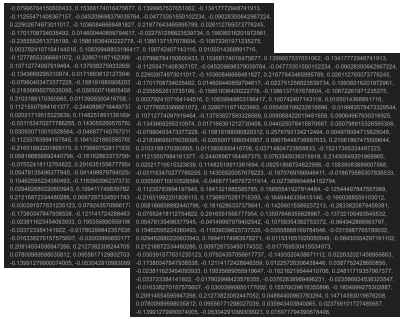








128 measurements



Compare with faces encoded

Where are the faces?

Will Ferrell? vs Chad Smith?

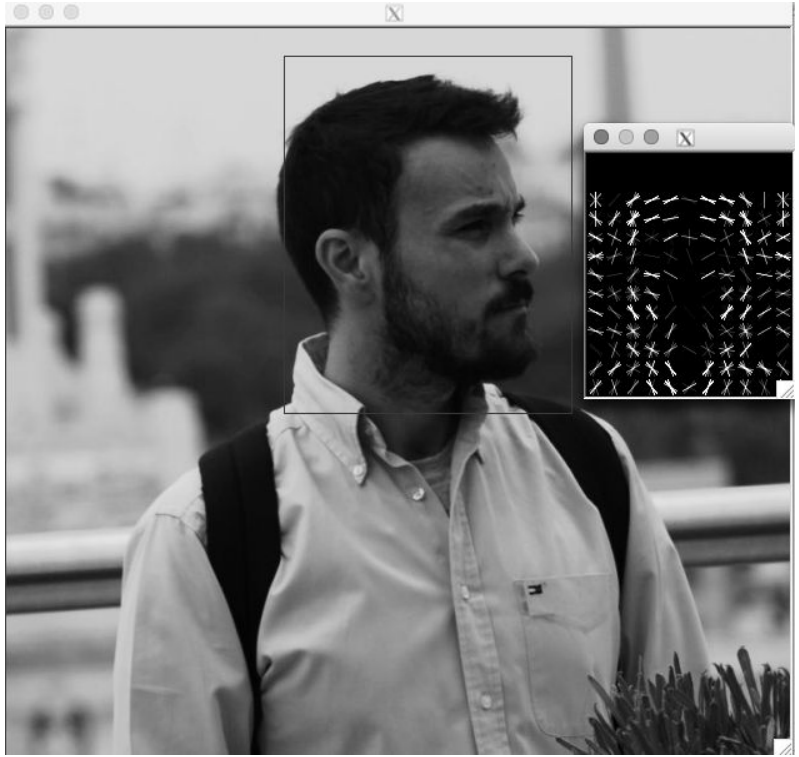
Difficult for humans too. Chihuahua vs muffins

Where are the faces? HOG. Histogram of Oriented Gradients

HOG. Histogram of Oriented Gradients

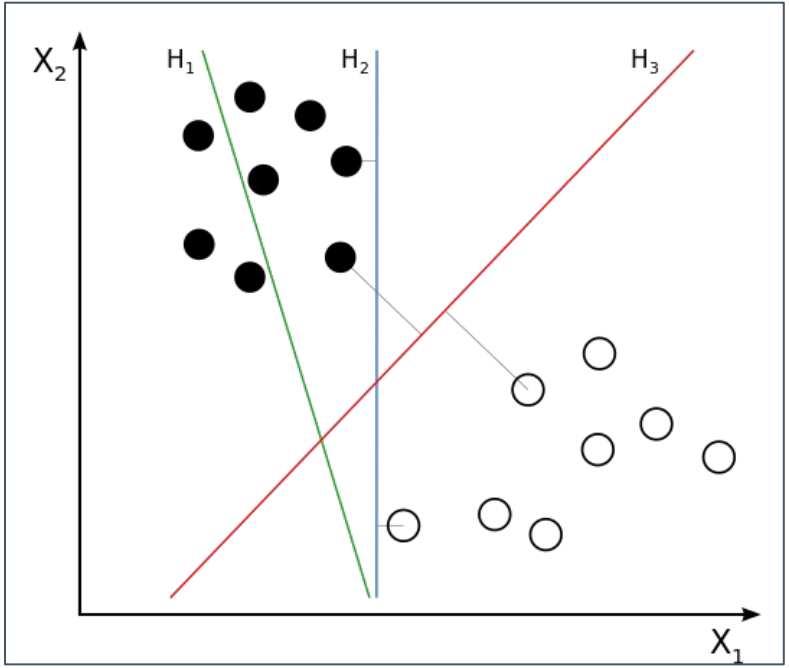
HOG: 2005. Navneet Dalal and Bill Triggs. Histogram of Oriented Gradients over human models

http://lear.inrialpes.fr/people/triggs/pubs/Dalal-cvpr05.pdf

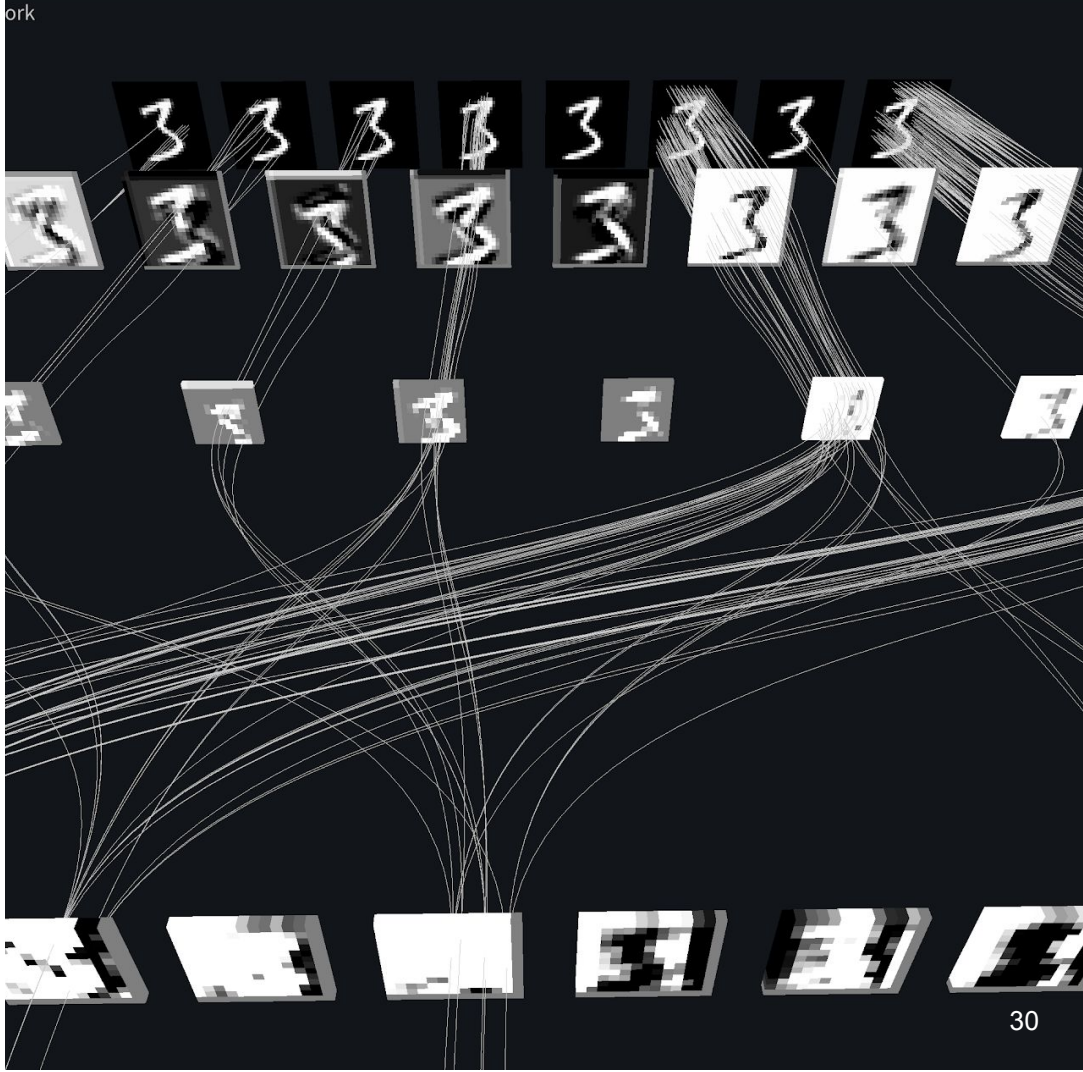


HOG Histogram of Oriented Gradients

Classification.
Support Vector
Machine
algorithm.



Where are the faces? CNN. Convolutional neural network



http://terencebroad.com/convnetvis/vis.html

CNN Convolutional neural network. Convolutions Kernel

Convolutional Border Kernel detections

255	255	255	0	0	0
255	255	255	0	0	0
255	255	255	0	0	0
255	255	255	0	0	0
255	255	255	0	0	0
255	255	255	0	0	0

X

1	0	-1
1	0	-1
1	0	-1

=

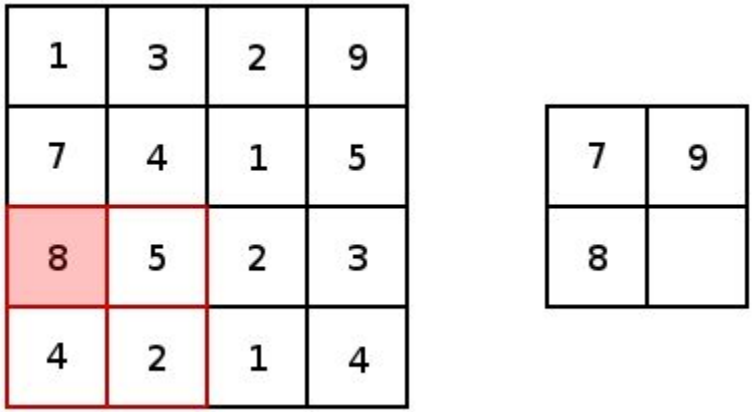
0	765	765	0
0	765	765	0
0	765	765	0
0	765	765	0

black hat EUROPE 2018

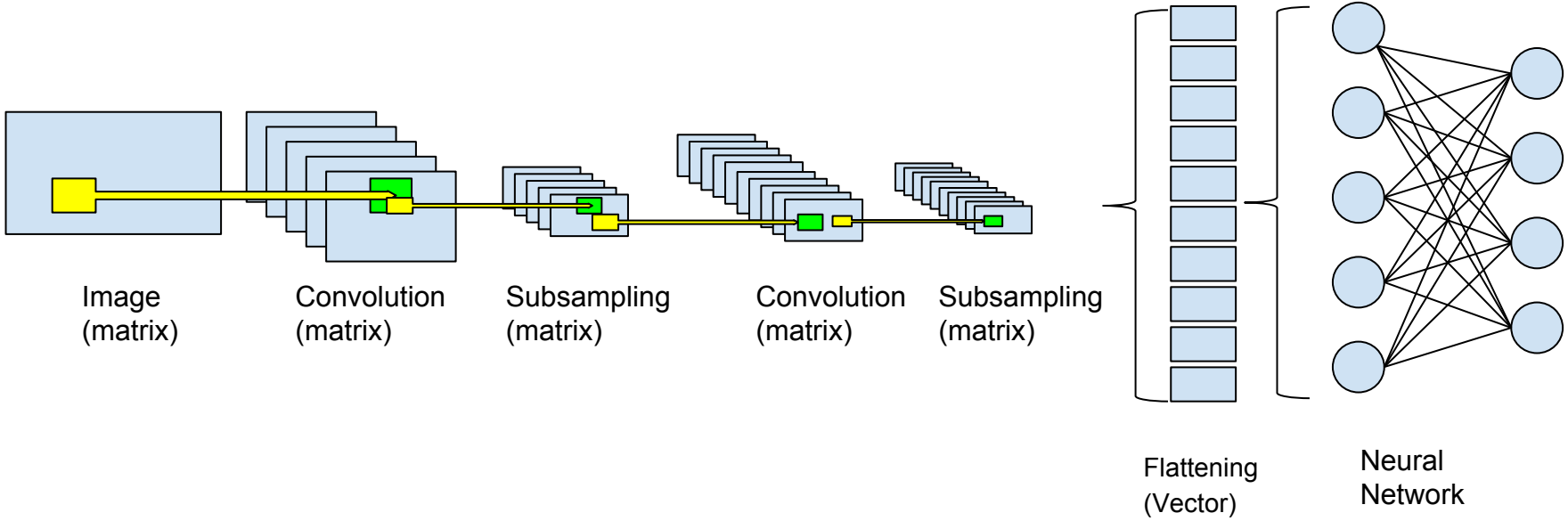
CNN Convolutional neural network. Filter Kernels

GIMP Example

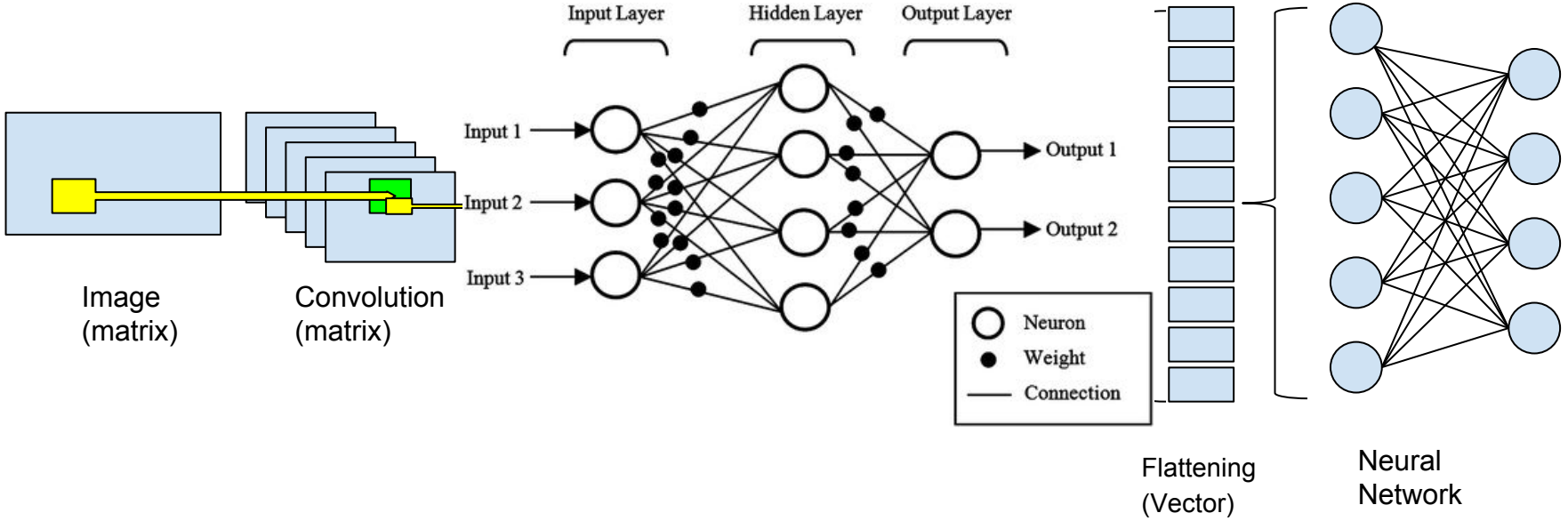
CNN Convolutional neural network. Subsampling Max Pooling



CNN Convolutional neural network



CNN Convolutional neural network



Caution

Don't use CNN in a CNN Video. The recursivity may cause world implosion

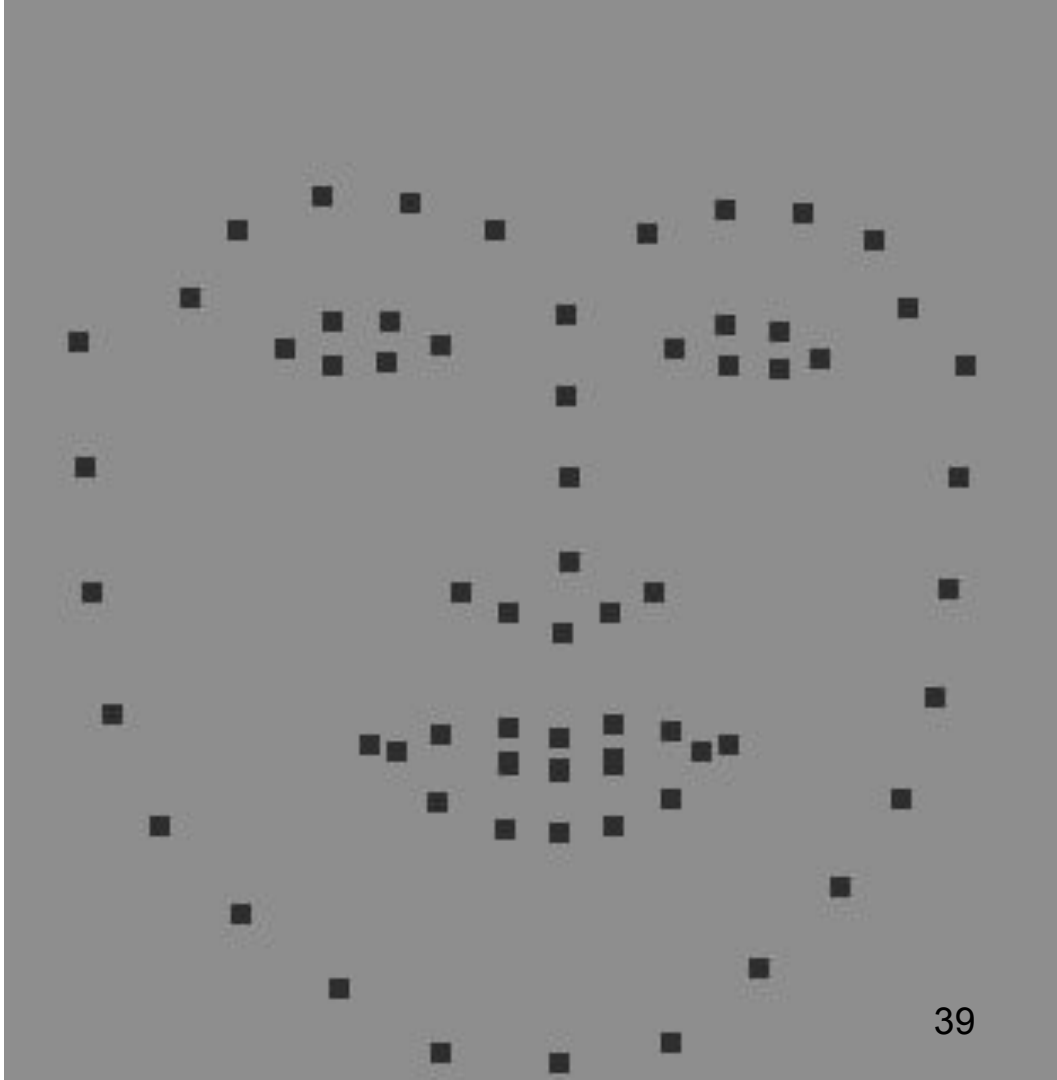
CNN + CNN =

CNN. More precise in object recognition.
(Processing offline)

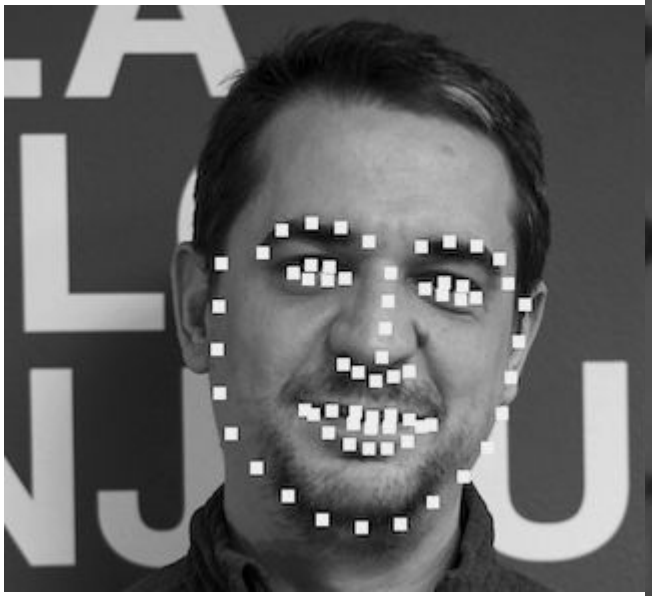
HOG. Faster in processing.
(Video in real time)

All that glitters is not ~~Gold~~ Faces

Face landmarks



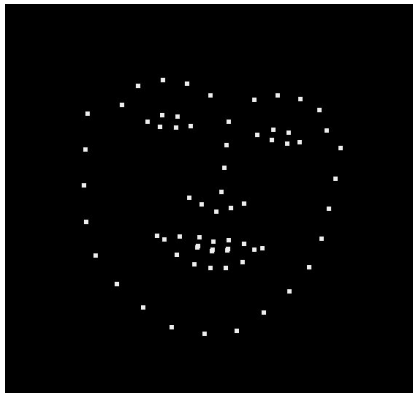
Face landmarks



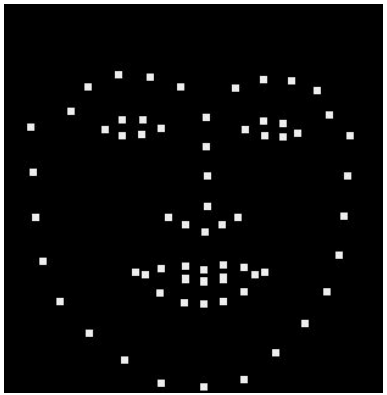
In this examples:
17 in chin
5 in left eyebrow
5 in right eyebrow
4 in nose bridge
5 in nose tip
6 in left eye
6 in right eye
12 in top lip
12 in bottom lip

2014 by Vahid Kazemi and Josephine Sullivan. http://www.csc.kth.se/~vahidk/papers/KazemiCVPR14.pdf

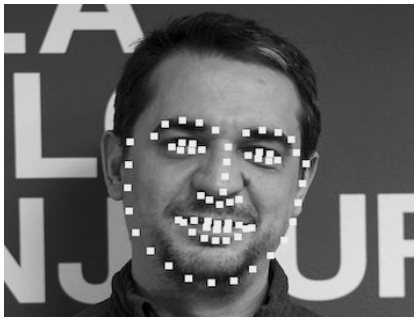
Align all landmarks with affine transformations: scale, rotate and shear



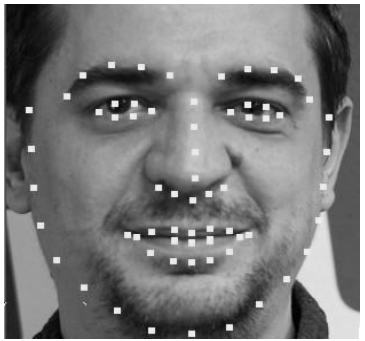
Obtain



Desired



Obtain



Affine transformation

Faces encoding

Faces encoding

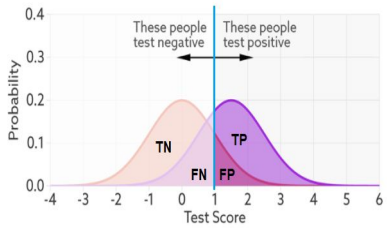
Create in 2015 by researchers at Google.

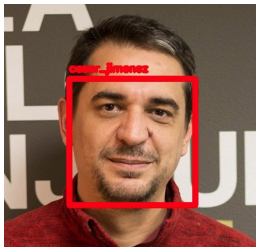
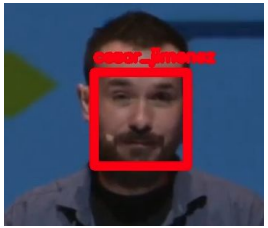
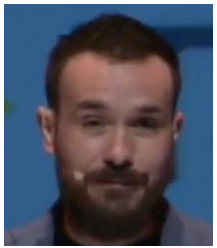
-0.07996784150600433, 0.15368174016475677, 0.1399957537651062, -0.13417772948741913, -0.11255471408367157,
-0.045209698379039764, -0.04773351550102234, -0.09028300642967224, 0.22902674973011017, -0.10360846668481827,
0.21877643465995789, 0.026112765073776245, -0.1701708734035492, 0.014600440859794617, -0.022751256823539734,
0.19936016201972961, -0.2355552613735199, -0.15861636400222778, -0.1386137157678604, -0.10872261971235275,
0.0037924107164144516, 0.10839948803186417, 0.100742407143116, 0.0105014368891716, -0.12778553366661072,
-0.3286711871623993, -0.055458199232816696, -0.019983578473329544, 0.10712774097919464, -0.13793827593326569,
0.009068422019481659, 0.09064967930316925, -0.1343669295310974, 0.017166361212730408, 0.044025078415870667,
0.050798915326595306, -0.07990403473377228, -0.15819168090820312, 0.2576793134212494, 0.004978094715625048,
-0.21836695075035095, -0.02650071680545807, 0.09678448736667633, 0.21061867475509644, 0.3103189170360565,
0.0113909300416708, 0.037148044723858833, -0.15217365324497223, 0.11215507984161377, -0.24408987164497375,
0.0763545036315918, 0.21450649201869965, 0.020217195153236639, 0.11482518911361694, 0.09251868724822998,
-0.15836083889007568, -0.031153470277786255, 0.14305520057678223, -0.1970769166946411, -0.018679585307836533,
0.030500710010528564, -0.046877145767211914, -0.027389904484152794, -0.11235783994197845, 0.1841321885585785,
0.15685541927814484, -0.12544497847557068, -0.21651992201805115, 0.17368975281715393, -0.1649446338415146,
-0.1660388559103012, 0.058186858892440796, -0.1616286337375641, -0.14266015589237213, -0.2833820879459381,
-0.07552418112754822, 0.2916351556777954, 0.13597646355628967, -0.13732105493545532, 0.05478135496377945,
-0.04149997979402542, -0.10759354382753372, -0.064942866563797, 0.15462595224380493, -0.11839039623737335,
-0.03558868169784546, -0.0315987765789032, 0.029462680220603943, 0.19941174983978271, -0.011531651020050049,
-0.08430354297161102, 0.21216872334480286, 0.009728733450174332, -0.017769530415534973, -0.030391577631235123,
0.07924357056617737, -0.1493520438671112, 0.022632021456956863, -0.17380347847938538, -0.12114172428846359,
0.01225726306438446, 0.0387752428650856, -0.023811623454093933, 0.19535689055919647, -0.18216219544410706,
0.24811719357967377, -0.033723384141922, -0.017802998423576355, -0.037628389896496231, -0.023586824536323547,
-0.016338270157575607, -0.03003990650177002, 0.15570029616355896, -0.1804899275302887, 0.20914554595947266,
0.21273823082447052, 0.04884400963783264, 0.14714393019676208, 0.07800989598035812, 0.09556171298027039,
0.035943403840065, 0.023756101727485657, -0.13991279900074005, -0.05304291099309921, 0.015071794390678406,
-0.022036418318748474, 0.07947075366973877, 0.10163198411464691

128 measurements of each face. Based on triplets.

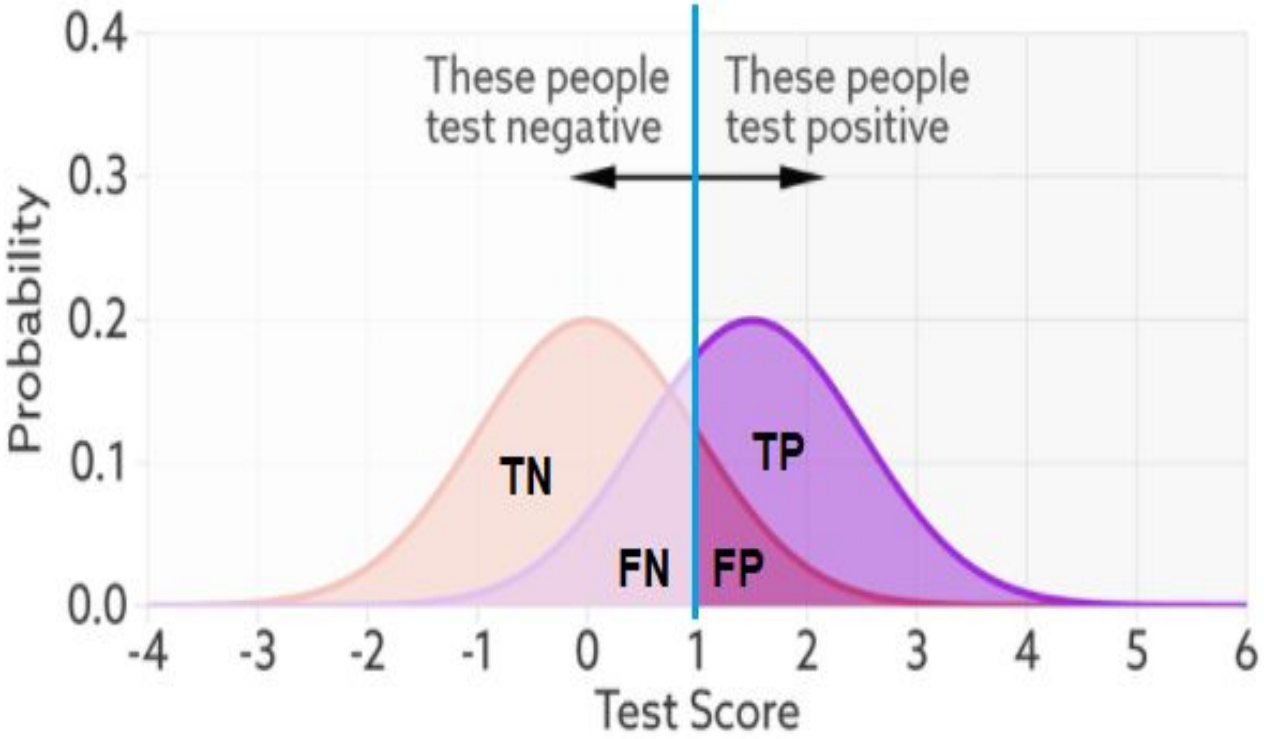
Face recognition

Determine tolerance.
Euclidean distance between vectors

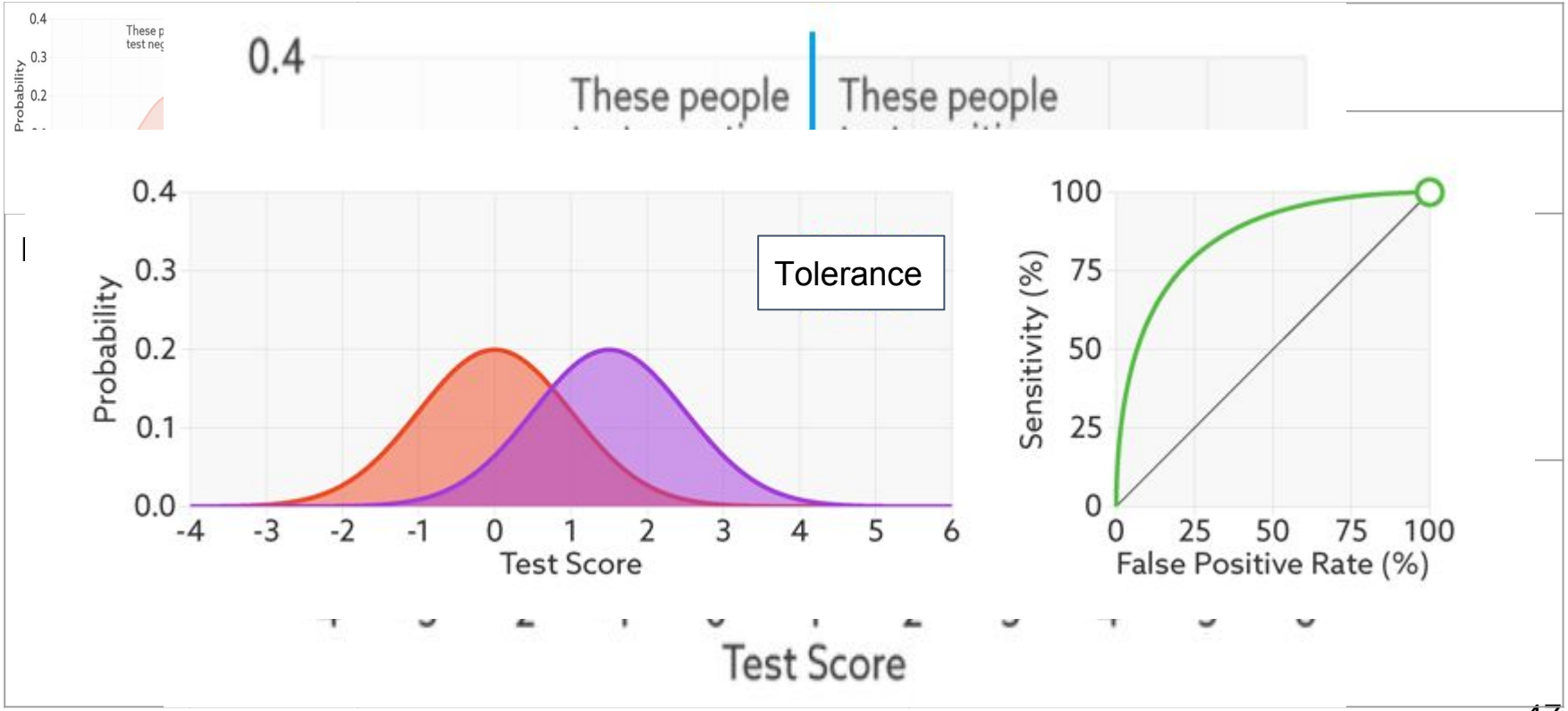


		Real	
		Positive	Negative
Prediction	Positive	TP 	FP 
	Negative	FN 	TN 

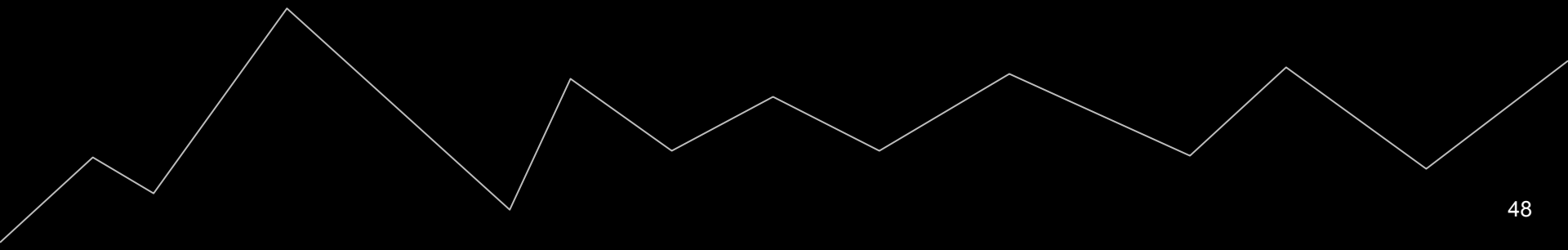
Determine tolerance.
Euclidean distance between vectors



Determine tolerance.
Euclidean distance between vectors



Unknown Unknowns



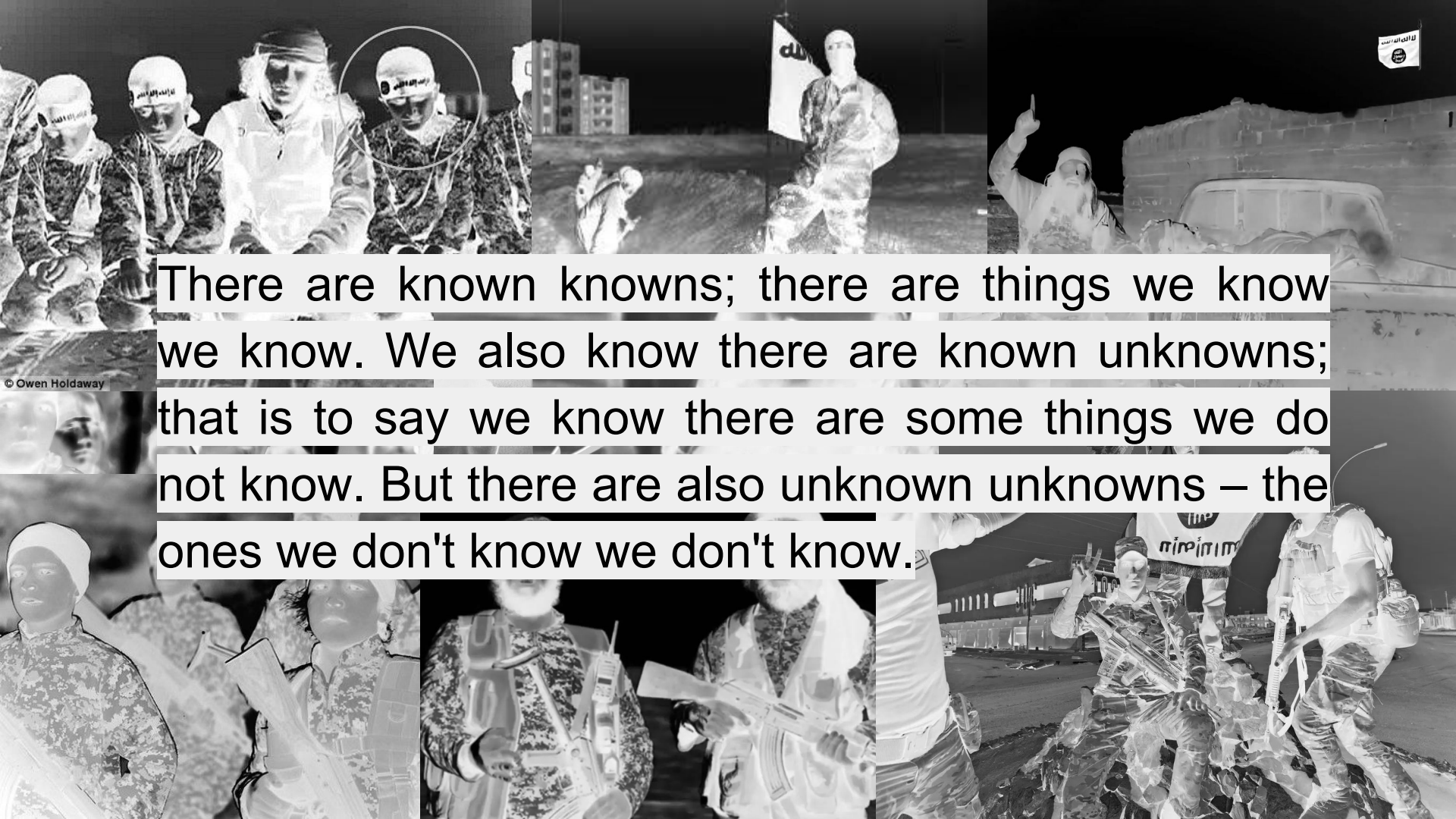
Unknown

Unknowns

COUNTER EXTREMISM PROJECT

From March 8 to June 8, 2018, the Counter Extremism Project (CEP) conducted a study to better understand how ISIS content is being uploaded to YouTube, how long it is staying online, and how many views these videos receive.

https://www.counterextremism.com/sites/default/files/eGLYPH_web_crawler_white_paper_July_2018.pdf


There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know.
© Owen Holdaway

Demo

Architecture

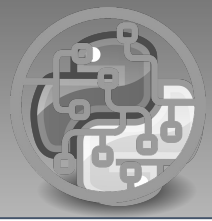
Do It Yourself

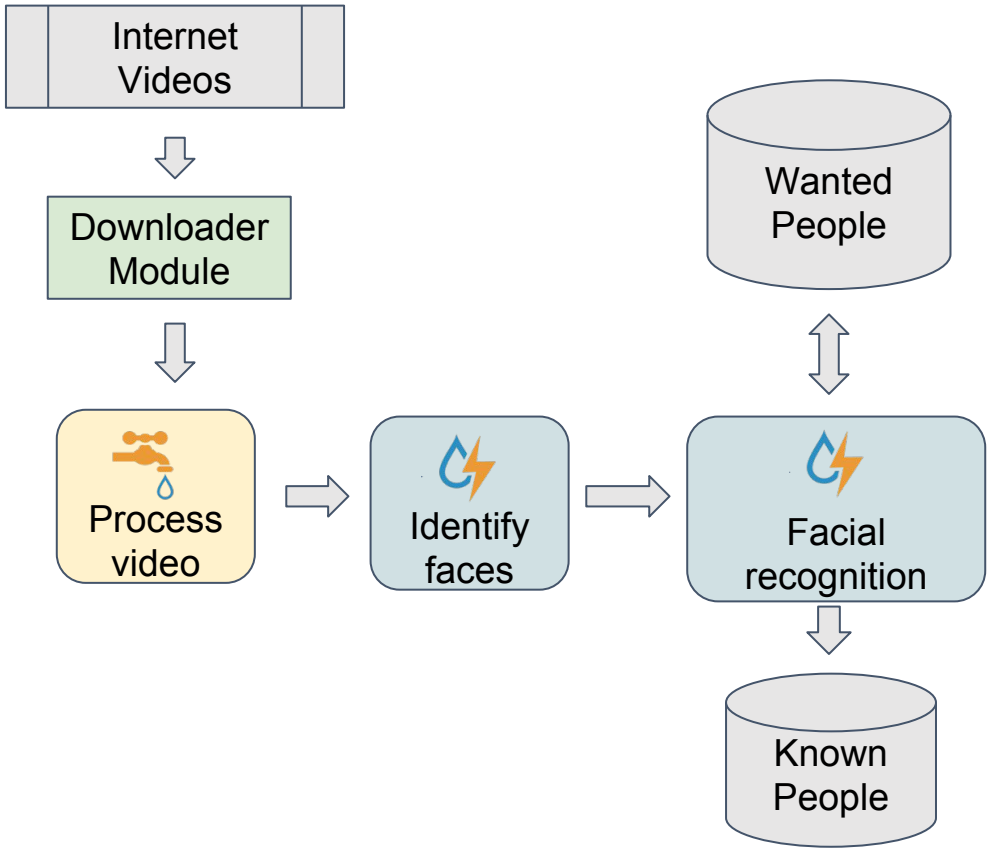
OpenCV (Open Source Computer Vision) is a popular computer vision library started by Intel in 1999.
https://opencv.org/

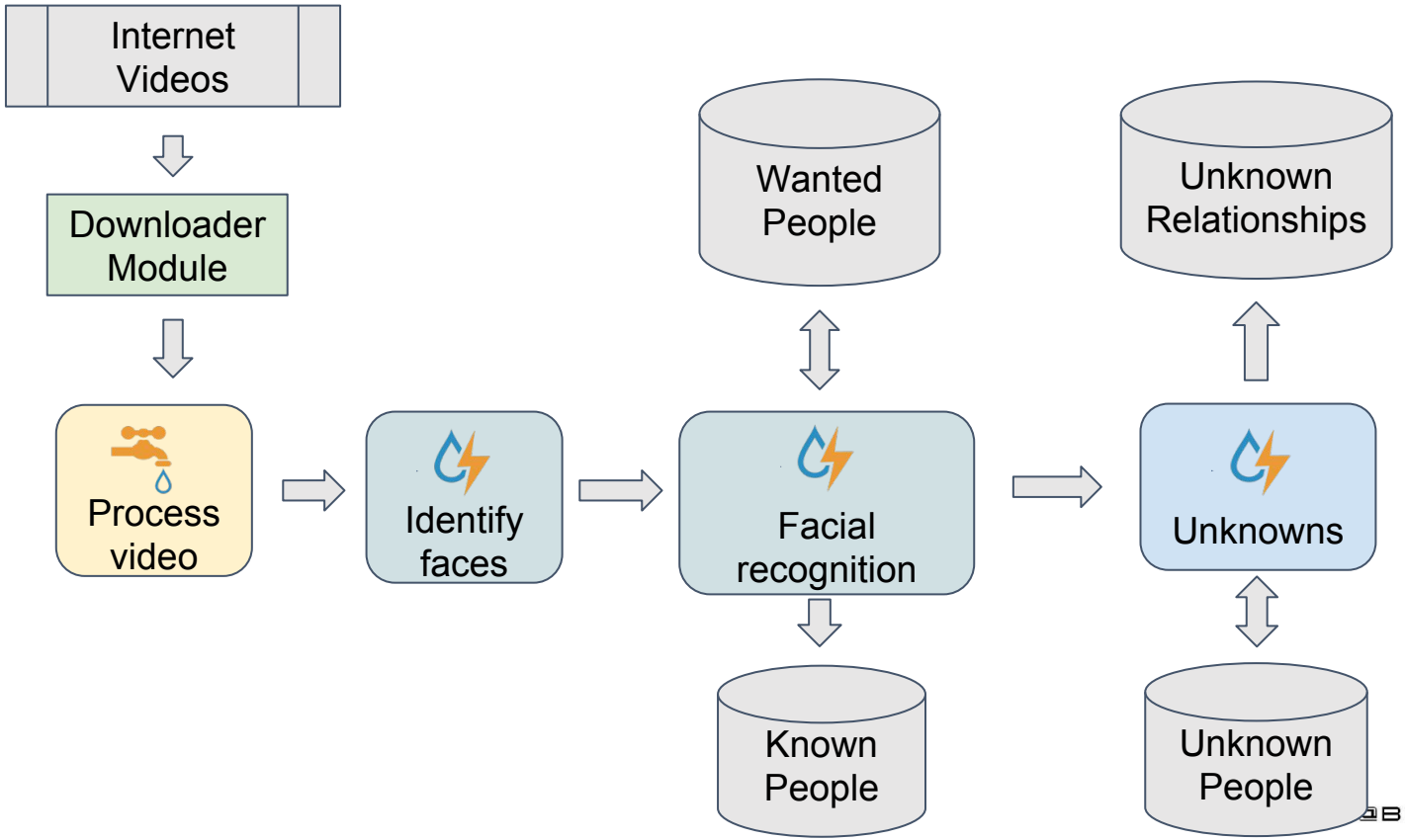
Apache Storm is a free and open source distributed realtime computation system.
http://storm.apache.org/

Dlib is a modern C++ toolkit containing machine learning algorithms and tools.
http://dlib.net/

Face Recognition. Recognize and manipulate faces from Python.
https://github.com/ageitgey/face_recognition




Internet Videos
Downloader Module
Process video
Identify faces
Facial recognition
Wanted People
Known People


Internet Videos
Downloader Module
Process video
Identify faces
Wanted People
Facial recognition
Known People
Unknown Relationships
Unknowns
Unknown People

How group Unknowns?

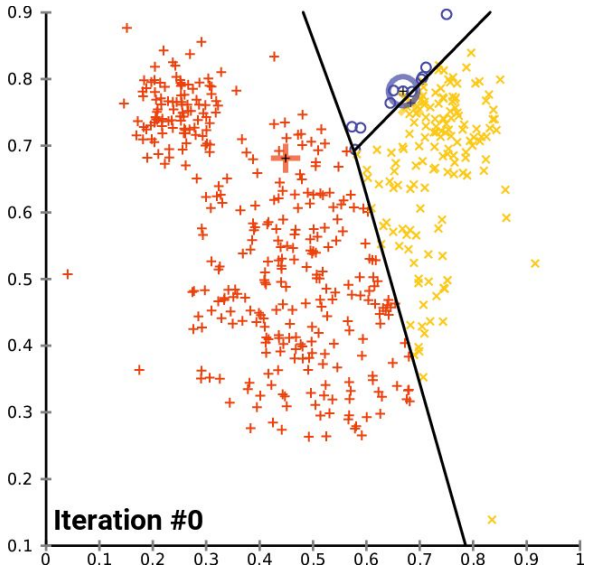
Hash similarity
or Perceptual
Hash
pHash

Don't work properly

Is influenced by
background, brightness,
face position ...

https://cloudinary.com/blog/how_to_automatically_identify_similar_images_using_phash
https://www.phash.org/

Clustering Model k-Means



Don't work properly

”Need” to know how many different persons are in the dataset

Convergence of k-means clustering from an unfavorable starting position (two initial cluster centers are fairly close). Generated with en:ELKI. Wikipedia contributors. (2018, October 3). K-means clustering. In Wikipedia, The Free Encyclopedia. Retrieved 19:22, October 3, 2018, from https://en.wikipedia.org/w/index.php?title=K-means_clustering&oldid=862308816

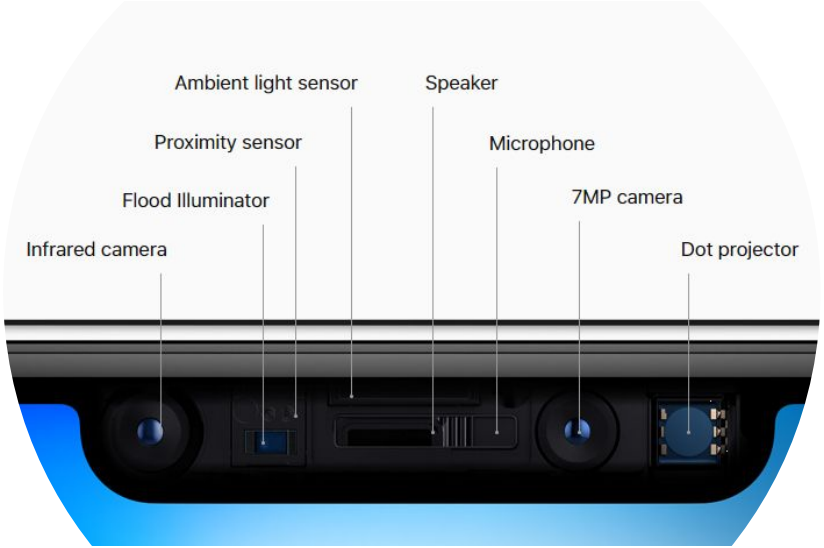
Chinese whispers

The algorithm works in the following way

- All nodes are assigned to a random class. The number of initial classes equals the number of nodes.
- Then all of the network nodes are selected one by one in a random order. Every node moves to the class which the given node connects with the most links. In the case of equality the cluster is randomly chosen from the equally linked classes.
- Step two repeats itself until a predetermined number of iteration or until the process converges. In the end the emerging classes represent the clusters of the network.

It works pretty well !!

Three-dimensional face recognition



Face ID

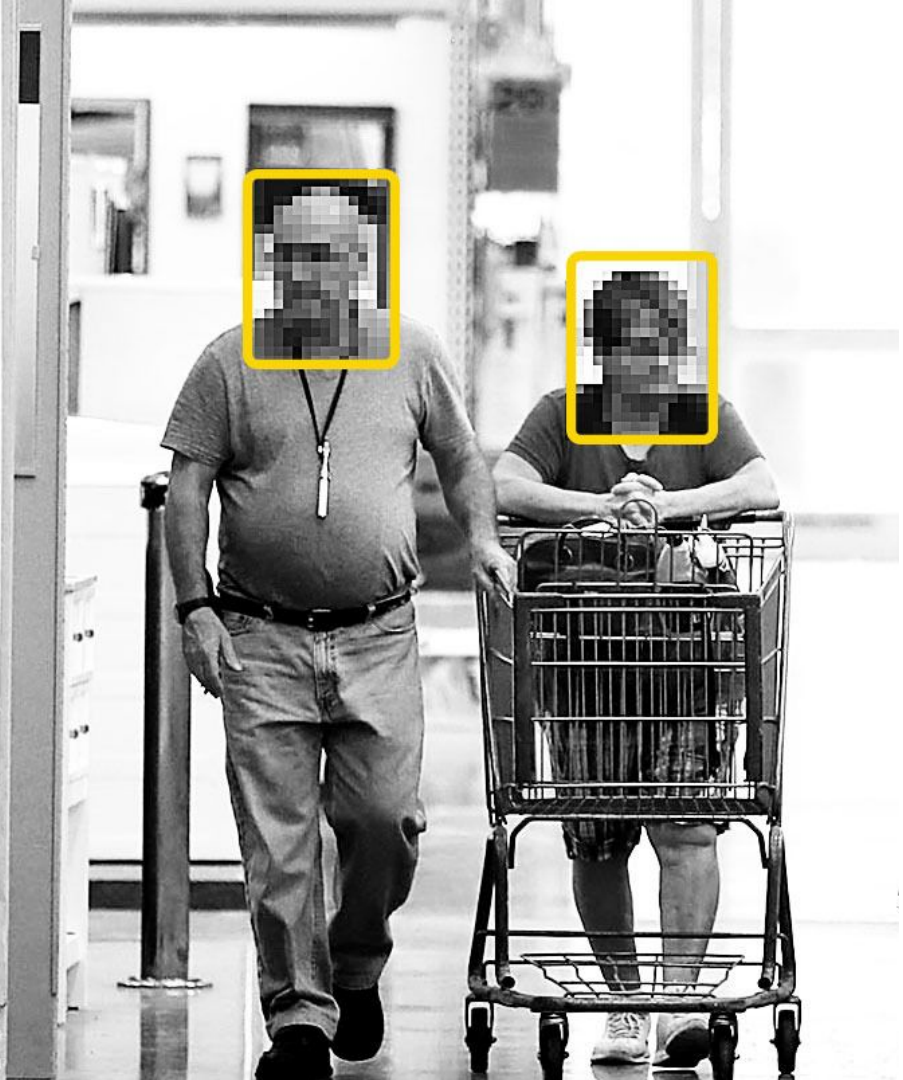
TrueDepth camera™

Intel®

RealSense™

Demo Epic {fail|win}

Social impact



Smile! The Secretive Business of Facial-Recognition Software in Retail Stores

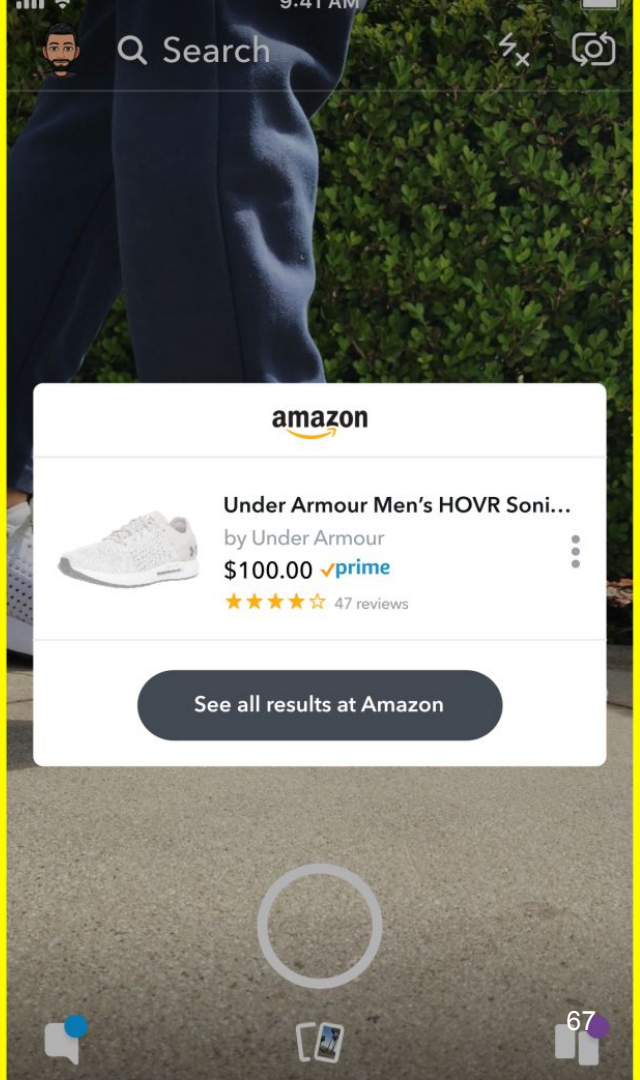
http://nymag.com/intelligencer/2018/10/retailers-are-using-facial-recognition-technology-too.html Photo-Illustration: Konstantin Sergeyev/Intelligencer; Photo: Joe Raedle/Getty Images

Tesla deploys massive new Autopilot neural net in v9, impressive new capabilities, report says

https://electrek.co/2018/10/15/tesla-new-autopilot-neural-net-v9/

Introducing Visual Search

https://www.snap.com/en-US/news/post/introducing-visual-search/



The world's first deep learning enabled video camera for developers

AWS DeepLens helps put deep learning in the hands of developers, literally, with a fully programmable video camera, tutorials, code, and pre-trained models designed to expand deep learning skills.

Buy Now

Register your DeepLens

Amazon

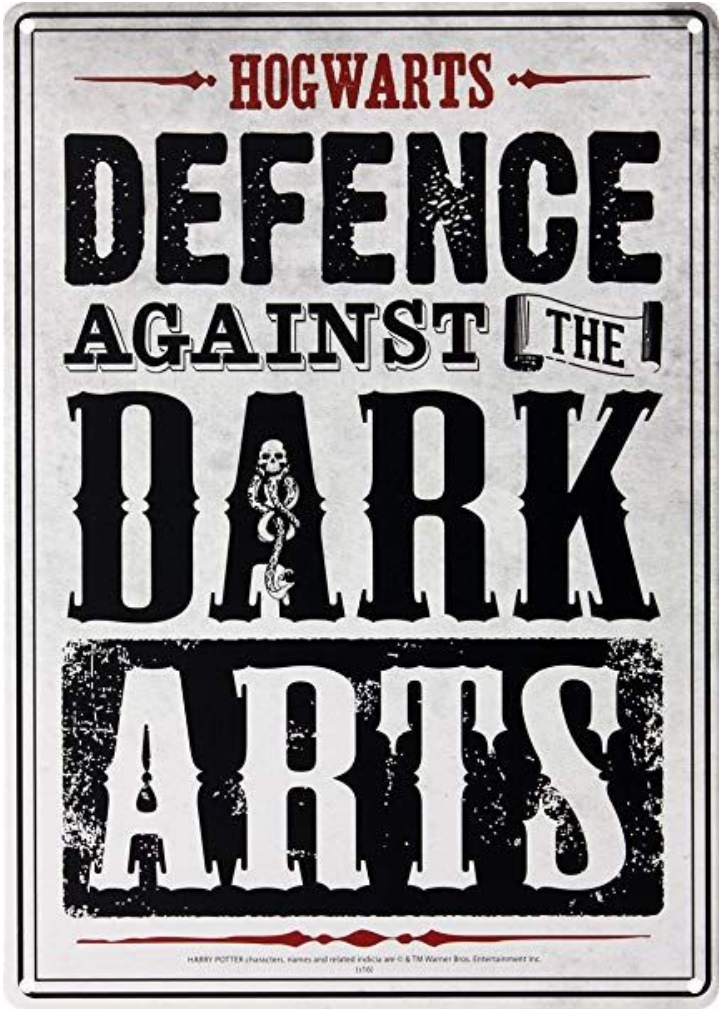
China's social score program coming to the world. 社会信用体系

“China's social credit system was launched in 2014 and is supposed to be nationwide by 2020. As well as tracking and rating individuals, it also encompasses businesses and government officials.”
https://www.wired.co.uk/article/china-social-credit

“Some types of punishments include: flight ban, exclusion from private schools, slow internet connection, exclusion from high prestige work, exclusion from hotels, and registration on a public blacklist”.
https://en.wikipedia.org/wiki/Social_Credit_System

Kevin Hong

Defence Against the Dark Arts



https://www.amazon.com/Harry-Potter-Defence-Against-Small/dp/B01DJNGUR6

Defense. Anti - facial recognition systems

Justice Caps

http://justicecaps.com/

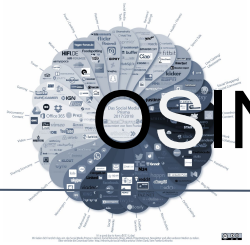
Defense.
Anti - facial recognition systems

https://www.kickstarter.com/projects/reflectacles/reflectacles-reflective-eyewear-and-sunglasses

Defense. Anti - facial recognition systems

https://cvdazzle.com/

Sound Bytes



OSINT Must Include Video Processing.

We've a Great State of Dlib Art.

If You're Afraid buy a  Mask.

Fran Gomez @ffranz
Cesar Jimenez @cesarjz

https://github.com/ffr4nz/UnknownUnknowns